HRWize in relation to Moorepay

At HRWize, we are committed to providing the highest level of service, security, and assurance to our clients. To provide greater clarity on the strength of the platform and services offered, the relationship between HRWize and Moorepay (acquirer of NaturalHR) is outlined below.

HRWize is a Canadian-based business that implements and delivers a white-labeled version of the Moorepay platform, a leading UK-based HR and payroll solution provider. Through this strategic partnership, HRWize leverages the full technical and security capabilities of the Moorepay platform while providing localized, bilingual support and services to Canadian organizations.

Both Moorepay (as the platform provider) and HRWize (as the service provider) maintain independent certifications under ISO/IEC 27001, the international standard for information security management systems. This dual certification ensures that not only the underlying platform but also the HRWize operational practices and service delivery processes meet the highest security standards.

To provide further transparency, the Moorepay Assurance Pack outlines the security framework, processes, and certifications in place to protect client data. Clients are welcome to request copies of the respective ISO 27001 certificates or any additional information as needed for their assurance processes.

This document, together with the ongoing commitment to security and service excellence, is intended to provide complete confidence in HRWize as an HR technology partner.

Document 1 - Introduction to the Moorepay Assurance Pack

Introduction

At Moorepay, information is our business, and the security of your data is paramount. We understand the obligations you have in ensuring the security of your data when entrusted to us and we are committed to working with you to provide the assurances that you require.

When evaluating a vendor for risks or performing annual due diligence activities related to information security, organisations have traditionally used questionnaires to gather information. The results gained by this approach often lack the context to fully

understand a suppliers security posture and ultimately do not provide the requisite knowledge for you to complete your supplier due diligence activities.

The Moorepay Assurance Pack (MAP) is a compilation of documents and artefacts designed to offer our customers a deeper insight into the Moorepay security practice.

The MAP includes independent attestations and certificates, along with documentation describing the technologies, processes and controls we have deployed to protect your data and meet the legal, regulatory and contractual requirements associated with data processing.

MAP content

The following documents and artefacts are included in the MAP.

Information Security Management System

The Information Security Management System (ISMS) is a framework of policies and procedures incorporating the administrative, technical and physical controls deployed by Moorepay to ensure that the confidentiality, integrity and availability of data is maintained.

This MAP document seeks to offer a concise summary of those policies, procedures and controls.

Data protection overview

An essential activity within Moorepay is the requirement to gather and process personal data about our client's employees, this is done in accordance with the applicable data protection and/or privacy laws of the countries in which we operate.

The General Data Protection Regulation (GDPR) is used as the best practice standard in countries where there is no equivalent data protection and/or privacy law or regulation.

Local legislation may require a specific implementation of policies and practices to align with local legal requirement(s). For UK based operations, Moorepay aligns with The UK General Data Protection Regulation (UK-GDPR)

This MAP document seeks to consolidate relevant information on the implementation of practices and policies adopted by Moorepay to ensure the secure handling of data in line with applicable laws and regulations as outlined above.

Business continuity

The Business Continuity MAP document seeks to provide an insight into Moorepay business continuity planning and provide a high level illustration of:

- leadership commitment
- the approach to business continuity planning and assessment
- the associated collateral
- impact assessments
- testing overview

Application security overview

The MAP includes documentation that describes the security features designed into Moorepay proprietary products (such as MoorepayHR aka HRWize) along with information on the security controls deployed across the underlying infrastructure and the physical security in place at the data centres.

Your MAP will include information on applications specific to your service provision.

Moorepay portal security overview

Moorepay Portal is our business to business digital platform available to Moorepay customers, offering a single, secure destination for customers to engage with our teams and processes.

The MAP documentation describes the security features designed into the product.

Certification

Copies of the following certificates can be provided upon request where the required confidentiality and none disclosure agreements are in place:

- ISO 27001:2013
- Cyber Essentials

Penetration test results

Moorepay contracts with independent third parties to conduct the following:

- Twice yearly infrastructure penetration tests
- Pre-release application penetration tests

The following information is available upon request where the required confidentiality and none disclosure agreements are in place:

- Third party executive summary report, providing an independent high level view of the scope of testing and the number and severity of vulnerabilities detected.
- Internally produced remediation attestation, providing a description of each vulnerability detected along with the associated remediation plan and target completion date.

Document 2 - Moorepay Information Security Management System

Introduction

This document forms part of the Moorepay Assurance Pack (MAP) and should be viewed alongside all other documents and artefacts included in the MAP to gain an overall understanding of the Moorepay security practice.

The Moorepay Information Security Management System (ISMS) is a framework of policies and procedures incorporating the administrative, technical and physical controls deployed by the organisation to ensure that the confidentiality, integrity and availability of data is maintained at all times, when entrusted to us.

This document seeks to describe those policies and procedures to give you the required assurance that good practice is being followed and that your information is secure.

The security measures mandated by the ISMS incorporate the following key security areas:

Risk management

Information security policies

- Organisation of information security
- Human resource security

Asset management

- Identity and access management
- Cryptography
- Physical security
- Operations security
- Communications security

- System acquisition, development and maintenance
- Supplier security
- Security incident management

Business continuity and disaster recovery

Compliance

For each key area there are a subset of security control requirements, and within those subsets we have described the measures implemented to ensure the security of your data, in terms of the policies mandating the controls and the practices deployed to deliver those policy objectives.

Risk management

Information security risk assessment

The implementation of the Company's information security risk strategy is based on formal and repeatable methods for risk assessment, risk management and risk acceptance.

Critical assets are categorised for risk assessment (e.g. vendors, IT infrastructure, data centres), and the associated threats, vulnerabilities and impacts considered. This is a broad assessment for each category of critical asset.

The identification of [security] risk can also be made from a number of activities, such as:

- security incidents and weaknesses.
- findings from internal or external [security] assessments and audits.
- new projects or significant changes to existing projects. (all projects that aim to handle confidential or restricted information are subject to a Data Privacy Impact Assessment).
- implementation of new products or services.
- appointment of a new supplier. (risk assessment is completed prior to the granting of access rights to third parties and must include a Data Privacy Impact Assessment when personal information is to be stored, processed or transmitted).
- an assessment of potential threats to the Company's activities and interests.
- changes in legislation affecting the Company's activities and interests.

It is the responsibility of all Moorepay employees to identify and report any risks in their area of responsibility to the designated risk owner. For security risks they will inform the Head of Security and/or members of the Security team who will assist with the assessment of risk.

Identified security risks are reviewed as part of a regular ISMS management review and where appropriate a formal risk assessment is undertaken by the Security Manager.

The risk assessment is documented and submitted to the CISO for review.

Risks are calculated using a 1-5 scale for impact (regarding confidentiality, integrity and availability of information assets/resources) multiplied by a 1-5 scale for vulnerability and 1-3 scale for probability.

Risk scored are established for gross risk (uncontrolled) and net risk (taking in to account current deployed controls and the effect they have on risk reduction).

Information security risk treatment

For each identified risk, a risk treatment plan is formulated and formally agreed by the risk owner (usually an extended leadership team member).

Risk treatment options are selected based on various considerations and include the following options:

- reduce – the level of risk is reduced to an acceptable level by the introduction of controls
- retain (accept) – the decision is made to retain the risk in its current form
- avoid – the condition that gives rise to the risk is avoided
- transfer – the risk is transferred to a third party

Information security policy

Management direction for information security

The objective of this subset of controls is to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Policies for information security

Moorepay has a documented Information Security Management policy which sets out the organisation's approach to managing its information security objectives.

The policy sets out Moorepay's strategic commitment to information security management that:

- ensures the continued quality of service
- meets the organisation's contractual, legal and regulatory obligations
- meets the needs and expectations of clients and other interested parties.

The policy ensures that information security management is treated as an integral part of management activities and is pursued in the same manner and with the same vigour as other managerial objectives.

The primary objectives of the Information Security Management policy are to:

- protect Moorepay and its clients' information assets from all threats, whether internal or external, deliberate or accidental
- minimise the risk of damage by seeking to prevent the occurrence of security incidents and reducing their potential impact.

The scope of the Information Security Management policy encompasses all forms of information security related to the Company's information assets, and information processing assets, business activities and information entrusted to Moorepay by its customers in all its forms, including data stored on computers, transmitted across networks, recorded on paper or held on other storage devices.

The policy establishes the minimum-security objectives to ensure that: information is only accessible to those authorised to have access, to ensure the information we process, and the methods used are accurate and complete and to further ensure that the information we process is available to all authorised stakeholders when it is required.

The Information Security Management policy is supported by a set of topic specific policies, standards, guides, processes and other documentation. A summary of this policy set is available upon request, subject to approval.

Where a Company information security policy or standard requirement cannot be met for any reason, a formal request for exception must be submitted in writing for approval. Failure to obtain exception approval will be considered a breach of this policy.

Any breaches of Moorepay information security policies may be subject to a formal security investigation and could lead to disciplinary action being taken against individuals.

All Moorepay security policies and standards are communicated to all employees and made available to other interested parties, as appropriate.

Review of the policies for information security

All information security policies and standards are reviewed at least annually unless changes to business operations, relevant legislation, regulations, contractual commitments or codes of practice necessitate an earlier amendment.

All information security policies and standards are reviewed and approved by the Head of Security.

For certain policies, further approval may be required by subject experts or department heads.

Organisation of information security Internal organisation

The following controls have been deployed to establish a management framework to initiate and control the implementation and operation of information security within Moorepay.

Information security roles and responsibilities

The Chief Information Security Officer (CISO) has overall accountability for Information and Cyber Security within Moorepay, reporting to the Chief Product and Technology Officer (CPTO), and with formal reporting lines to the Chief Executive Officer (CEO), ensuring executive oversight.

The Security Leadership team reporting to the CISO is responsible for information and cyber security functions and services within Moorepay, A dedicated team of security specialists (Security team) report into the leadership team to deliver the information and cyber security practice.

Moorepay also has in place a Managed Security Services Provider (MSSP) providing additional security services, such as threat intelligence, SIEM and SOC services.

The Legal team and Compliance & Auditing team report into the General Counsel. Key roles and responsibilities are as follows:

- The CEO and Senior Leadership Team have overall responsibility for the Company information security strategy.
- Compliance team is responsible for managing the ISO certifications programme which forms part of the Company compliance activities.

- Compliance and Data Privacy team ensure that relevant legislation is tracked and that business managers are made aware of changes in legislation.
- Moorepay business areas have appointed Security Champions to support the
- ISMS management process, the deployment of policies and to help with security awareness.
- HR security is the responsibility of Company HR team and line management. Preemployment screening is completed utilising the nationally recognised standard. where specific customer contracts require enhanced vetting, this is undertaken by the business units via the appropriate authorities.
- Annual Compliance Training (ACT) is owned by the Compliance team. The objective is to make sure that all Moorepay employees understand Company policies (including security and data privacy policies).
- Compliance and Data Privacy team is responsible for ensuring that Moorepay complies with the data protection legislation in the UK and Ireland.
- Shareholders with independent, objective assurance that appropriate internal controls are in place, are robust and are being complied with. The Internal Audit team facilitates an annual assessment of the Company security management system.
- Physical security policy and standards for Company buildings is owned by the Head of Security and Facilities Director.
- IT security and network security management functions are owned by the Product and Technology business area with various specialist IT teams supporting the businesses. Solutions, including the evaluation and purchase of
- IT security products including AV, intrusion detection, firewall, data encryption etc., are agreed with the Information Security team before deployment and implementation.

Segregation of duties

Moorepay has a documented segregation of duties policy. The policy details the requirements around roles and responsibilities to reduce the reliance on key individuals and to prevent errors, and fraud as a minimum.

The policy mandates that, adequate segregation of duties and control responsibilities must be established and maintained in all functional areas of Moorepay. In general, custodial, processing/operating, and accounting responsibilities are kept separate to promote independent review and evaluation of Moorepay operations.

The following are examples of job functions which must adopt segregation of duties.

- Systems administrators must not carry out security administrator functions. The authorisation for creation of administrator accounts must be recorded.
- Network administration function must be a separate function to that of infrastructure management. This will ensure that end to end access to data (including sensitive data) is only possible through collusion and therefore reduces the risk of misuse of
- Moorepay's information facilities.
- Employees engaged in finance roles must not be able to complete all stages of any transaction. E.g. employees must not be able to create, approve and complete all stages of a transaction.
- Database administration and infrastructure system (e.g. server host administrator) activities must not be performed by the same person or team.
- Security administrators must have no access to database administration privileges.
- Software development and maintenance staff must have no cross access to computer operations (production environments) including database administration, network administration and system (Infrastructure) administration.
- Security administrators and firewall administrators must have no privileged access accounts on infrastructure production systems (e.g. operational roles), except security technologies/firewalls, IDS/IPS etc.

Legal & Regulatory updates

Moorepay's Product teams monitor relevant regulation and statutory impacts to the services and products we offer including in the areas of labour and employment, payroll, benefits, global mobility, recruiting, and data privacy and protection, among others.

Moorepay's Compliance team monitors and track corporate legal and regulatory obligations including those requirements relevant to the ISMS.

Contact with special interest groups

Our product strategy plan is influenced by the HR and payroll marketplace, industry trends, changes in technology, but more importantly, our customers, through our user groups and special interest groups.

Moorepay receives threat intelligence and other security information from various sources, including but not limited to the following:

- information on vulnerabilities and software updates from key vendors
- subscription to National Cyber Security Centre – Cyber Information Sharing Partnership (NCSC CISP)
- Bitsight cyber security ratings
- Digital Shadows threat intelligence platform
- Threat Intelligence from our Managed Security Services Provider (MSSP) via the Security Operations Centre (SOC)

Subscription to various special interest groups and forums specialising in security information is also done on an ad hoc basis throughout the Security team, technical teams and management tiers. Clear lines of communication are available for reporting concerns and advising of new threats to the Security team.

Information security in project management

The Technical Advisory Board (TAB) validates proposals for new technology. The Security team involvement in the TAB process ensures:

- the incorporation of security & privacy controls into proposed solution compliance with security and privacy policies
- satisfactory completion of data security and privacy assessment as evidence of compliance with security and privacy requirements

Security team representatives attend weekly planning and review sessions (ship rooms) to ensure that Security are appraised of all upcoming application development and infrastructure changes and are able to advice on potential risk points and security best practice.

Mobile devices and remote working Mobile device policy

The Moorepay Mobile Computing and Home Working Security policy covers the requirements for mobile device use. This policy applies to all employees and third

parties using mobile devices (which are taken to mean mobile phones, tablets, laptops, macs or other easily transportable computing equipment) and who are provided with authorised access to information and information processing systems.

- Employees must ensure the Moorepay Acceptable Use of Information Systems policy and Standard for Handling Information is applied when using mobile devices.

- All devices that are permitted to connect to and access information on the networks must have appropriate mobile device management solution applied to enable them to be remotely managed and data wiped if necessary.
- Mobile devices must be protected with approved encryption software. Passwords must comply with the Moorepay User Password policy.
- Employees must not permit any unauthorised user to access a Moorepay device, this includes family members.
- Employees must:
- Keep mobile devices used for business purposes hidden when not in use and not store Multi-Factor or any other supplied authentication devices alongside mobile devices used for access.
- Keep mobile devices in their possession and within line of sight whenever possible, taking care in public places such as airports, railway stations, hotels or restaurants.
- Take extreme care to protect confidentiality and minimise risk of exposure by limiting information that can be seen by others.
- Ensure that any confidential conversations /phone calls are taken in private areas, away from other people. Headphones/earphones must be worn to support privacy of work conversations.
- Turn off the Bluetooth facility when not essential and/or set to “hidden” to avoid calls being intercepted.
- In the event of a mobile device being lost or stolen, report it to the
- Moorepay Service Desk immediately to ensure the account is disabled and data wiped.

All supplied laptops have standardised secure builds deployed, which include the following:

- anti-malware software
- personal firewalls.
- whole disc encryption
- end user functionality controlled by group policy (e.g. no administrator access or ability to install software)

All mobile phone devices have whole disk encryption deployed and pin, or passwords use enforced. Access to information and systems is not permitted until these mandated security controls are confirmed.

Moorepay has deployed a Mobile Device Management (MDM) and Mobile Application Management (MAM) service to enable the centralised management of corporate mobile

devices. The service functionality includes but is not limited to the following mobile security components:

- remote wipe of the device
- deployment of security policies
- deployment of software
- confirmation of software levels and security policies
- prevention and control of access to Moorepay information and systems

Remote working

The Moorepay Mobile Computing and Home Working Security policy covers the requirements for remote working.

All employees working from home or other remote locations must ensure that information and devices are used in a manner compliant with:

- the Moorepay Acceptable Use of Information Systems policy.
- access control policies and standards.
- relevant information classification policies and procedures.
- all legal and regulatory requirements.

When working from home or remotely, employees must comply with the following minimum requirements.

- Take extreme care when using public wireless networks or those supplied in, for example, hotels, coffee shops or conference centres. Employees must ensure that they maintain privacy in such circumstances and to ensure connections are appropriately encrypted and secured.
- Implement appropriate privacy measures to reduce the risk of information being inadvertently disclosed to onlookers or neighbours (for example, through windows, open doors and overheard conversations) or whilst working in public spaces such as trains, planes, restaurants or bars.
- Ensure compliance with all relevant Moorepay health and safety policies and procedures.
- Ensure compliance with all relevant legal, regulatory, internal and contractual requirements.
- Dispose of information and devices securely and in compliance with the

Moorepay Secure Waste Disposal policy

- Keep Company printed documents out of sight and secure.
- Staff must not connect to Moorepay from a home network unless approved security controls are in place such as malware and firewall requirements.
- On termination of employment the Moorepay leaver process must be complied with and all equipment and information must be returned.
- Moorepay may undertake security audits and security monitoring.
- All staff working remotely must ensure a regular backup of information is undertaken and backups are protected with such as encryption.
- Only authorised users are permitted to work from home.

Technology is deployed to restrict access to the corporate network, local agents are installed on connecting devices that are integrated with Moorepay 's Active Directory. Devices used to connect must have the required configuration to authenticate, which along with user authentication offers pseudo 2 Factor Authentication (something you have and something you know). The software checks the connecting device to ensure it is compliant with corporate policies before allowing the connection to be established.

The software establishes an encrypted Virtual Private Network (VPN) connection between the connecting device and the corporate network.

Corporate standards exist and must be adhered to for the handling and disposal of information when working from home.

The ability to add personal printers to corporate devices is restricted and home printing must be authorised and enabled. Printing resources within Service Centres are utilised where possible to limit the amount of offsite printing and storage of hard copies of information.

Users who have been granted the ability to print must abide by the Moorepay Information Handling standard and where required, are supplied with specialist equipment to store and destroy hard copies of information.

Human resource security

Prior to employment

The following controls have been deployed to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Screening

Employee screening is mandatory before granting them any access to corporate assets. Background verification checks on all candidates for employment, contractors, and third party users are carried out in accordance with relevant local laws, regulations and to the business requirements.

Moorepay standard vetting requirements are;

- right to work check
- proof of residency check
- financial probity check
- five years of activity history
- criminal record check

Dependent on the role of the employee, additional checks are carried out in line with our client's contractual requirements for specific clearance requirements.

If a candidate fails one of the following checks then the Moorepay policy is that it must not hire:

- right to work
- unsatisfied CCJ's
- unspent convictions (with the exception of road traffic offences, unless these have resulted in disqualification and a valid licence is required to carry out their role).

If the candidate fails any other check then further review would be undertaken by HR and relevant stakeholders and a decision made on how to proceed on a case by case basis.

Terms and conditions of employment

As part of the employment obligation, employees, contractors and third party users must agree and sign the terms and conditions of the employment contract, which state their and the organisation's responsibility for information security.

The standard contract of employment includes but is not limited to the following clauses:

- Transfer of Technology
- Conflict of Interest
- Conduct and Duties
- Confidential Information
- Data Protection

- Non-Competition and Non-Solicitation
- Employee Monitoring

Any failure to adhere to the terms and conditions of employment is dealt with by Moorepay's own disciplinary process appropriate for local legislation.

During employment

The following controls have been deployed to ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Management responsibilities

Business divisions and local departments are responsible for creating appropriate procedures and work instructions to align with the corporate policies and standards.

Managers are responsible for ensuring that each employee within their scope completes and passes the annual security and compliance training, and that where required, additional training is provided to ensure employees have the required knowledge to do so.

Managers are provided with additional training to ensure that they understand their and their teams requirements regarding information security.

It is the responsibility of managers to initiate formal investigation where it is suspected that an employee is not meeting their requirements regarding information security.

Information security awareness, education and training

An e-Learning security training framework is provided, and completion annually is mandatory for all employees without exception. This is also part of the employee induction process and must be completed within 4 weeks of joining.

The objectives of the e-learning training framework are as follows:

- adhere to Moorepay security policies and standards
- participate in Moorepay business continuity and disaster planning
- understand key data privacy concepts important to the performance of your role
- comply with Moorepay anti-corruption and corporate compliance policies
- abide by Moorepays' approach to encouraging equality, diversity and dignity
- accept collective responsibility towards health and safety at work

All staff are tested on their knowledge of each subject and must attain an 80% pass mark to complete each module.

The training material is reviewed at least annually.

To supplement the annual training, the security team regularly deliver additional material focused on important aspect of security, providing further guidance on how to apply good practice and working in a more secure way.

Additional training needs are identified through a skills matrix which is updated on a regular basis. Training undertaken is captured in the performance review system.

Local divisions and departments are responsible for creating appropriate procedures

and work instructions to ensure that processing and support activities are undertaken in a consistent manner and in line with applicable corporate policies.

Disciplinary process

A formal disciplinary policy has been established by Moorepay to encourage all employees to achieve and maintain standards of conduct, attendance and capability. This policy enables the Company and its representatives to act effectively, consistently and fairly when dealing with such matters as misconduct, poor attendance an incapability.

Moorepay reserves the right to implement the disciplinary procedure at any stage as set out in policy, taking into account the alleged actions of an employee.

This applies to all employees who work for Moorepay or any of its subsidiaries in the UK and Ireland. It applies to all permanent and temporary staff as well as contractors.

Disciplinary action may be taken due to misconduct or incapability.

Investigations are conducted by appropriate management and Human Resource (HR) representatives.

Disciplinary action is determined based on the outcome of the investigation and in line with corporate policy.

Termination and change of employment

The following controls have been deployed to ensure that information security

requirements are understood and that Moorepay and its customers information is protected when the termination is carried out.

Termination or change of employment responsibilities

The Moorepay Leavers policy is enforced to ensure that employees responsibilities after termination are highlighted. As a minimum:

- all assets are returned, and the leavers manager submits a clearance form allowing for final payment.
- access is revoked, and user accounts disabled at the required time and date.
- an exit interview is performed, and the leaver has to sign a confidentiality agreement reiterating that they will maintain the confidentiality.

Asset management

Responsibility for assets

The following controls have been deployed to identify organisational assets and define appropriate protection responsibilities.

Inventory of assets

A CMDB or register is used to record and manage asset details. A combination of auto discovery and manual intervention by asset owners is used to maintain the records.

IT assets are recorded in the IT service management system, recorded information includes the following:

- asset name
- asset number
- asset type (e.g. server, laptop, router)
- designated owner
- status (e.g. production, development, awaiting disposal)

Ownership of assets

All information assets processed within Moorepay have an appointed Information Asset Owner (IAO) who must be a senior/responsible individual involved in the running of the relevant business function.

Their role is to understand what information is held, how information is received, removed and retained, and who has access and why. As such, they can recognise the value and lifecycle risks to their information assets and ensure that they are processed in accordance with Moorepay's security policies.

IAOs formally contribute to the assessment of risks to the confidentiality, integrity and availability of their information assets.

Responsibility for implementing day-to-day controls relating to their information assets may be delegated but accountability remains with the nominated IAO. For the purposes of applying information classification, an IAO may also be the author, creator or recipient of an item of information.

Acceptable use of assets

An Acceptable Use of Information Systems policy is part of the Moorepay Information Security policy framework. The aim of this policy is to state the requirements to ensure that security controls are applied, to protect Moorepay systems that store or are used to access information. Therefore, what is stated as acceptable use is defined to provide assurance to all Moorepay stakeholders that information is suitably protected.

It is mandated that Information security incidents (where unacceptable use of systems is suspected or has occurred) must be reported [immediately] using the information security incident reporting procedure.

Access to Moorepay systems must not be attempted without proper authorisation (following Moorepay access control requirements).

Moorepay monitor the use of Moorepay information systems for security purposes. The Acceptable Use of Information Systems policy covers the following areas:

- general use of Moorepay information systems
- protecting confidential or restricted information
- secure use of the Internet
- secure use of electronic communications
- physical security
- passwords
- removable storage media
- acceptable use of software
- secure configuration of Moorepay information systems
- monitoring of Moorepay information systems

The Acceptable Use of Information Systems policy follows associated controls set out in the following Moorepay policies and procedures:

- Mobile Device & Remote Working policy
- Clear Desk/Clear Screen policy
- Password policy
- Cryptography policy

Information Security Incident Reporting procedure

Return of assets

A Global leavers policy is enforced to ensure employees responsibilities after termination are highlighted.

The allocation of assets is tracked within the corporate ticketing system, the leavers process triggers the creation of a child ticket for local IT support to engage with the leavers line manager and ensure that all assets are identified and returned.

Only when all assets are returned, the leavers manager submits a clearance form allowing for final payment.

Information classification

The following controls have been deployed to ensure that information receives an appropriate level of protection in accordance with its importance to Moorepay.

Classification of information

Moorepay has a documented Information Classification and Ownership policy. The objective of the policy is to identify and implement adequate and effective information handling and protection controls, appropriate to the sensitivity of the information being handled. The purpose being to ensure that the valuable business and personal information used within Moorepay and the information entrusted to the organisation by its customers is appropriately protected throughout its lifetime.

All information generated must have a classification category applied.

This policy applies for both users (includes employees, employees of temporary employment agencies, vendors, business partners, contractor personnel, and customers) and corporate-owned systems processing any type of sensitive information and extends to information held in both paper and electronic formats.

This Policy is supported by the Information Handling standard which outlined the rules for handling information throughout each stage of its lifecycle.

The following principles shall apply to all information assets managed by or on behalf of Moorepay:

- the classification of an information asset must denote its suitability for release outside of the organisation and convey the security protection and handling needs when processing information internally.
- all major information assets must be accounted for, recorded and have a nominated Information Asset Owner (IAO) assigned to ensure that proper protection is maintained.
- the level of control to be exercised must be based on the classification of information as detailed below.
- Information Asset Owners and employees must:
- classify information assets and information processing facilities in accordance with this policy.
- appropriately label information assets and information processing facilities with its classification.
- handle and protect information in accordance with its classification and in line with client requirements and Moorepay's associated Information Handling standard.

Information must be classified to one of the following four categories:

- Public
- Information that is freely available. This is identified where no document label is present or by any document label that has none of following classifications.
- Company restricted for internal use only
- Information classified as Company Restricted for internal use can be released to any Moorepay employee or authorised and approved contractor. In some circumstances information under this classification may be released to third party organisations where a Non-Disclosure Agreement exists between the parties and Moorepay.
- Company or client confidential
- All personally identifiable information handled, processed or stored by Moorepay or on behalf of Moorepay, or entrusted to Moorepay by its customers.
- Company secret
- Information which if released would have a significant impact on Moorepay's reputation and commercial success.

The classification must be based on:

- legal requirements (which may affect confidentiality, integrity and/or availability controls),
- value and criticality (affecting integrity and/or availability controls)
- sensitivity to unauthorised disclosure or modification (affecting confidentiality controls).

Labelling of information

In line with Moorepay Information Classification and Ownership policy and associated Information Handling standard, the following controls are stipulated:

- Information Asset Owners (IAO) and employees must appropriately label information assets and information processing facilities with its classification.
- information must be classified and labelled in line with the Standard for Handling Information to reflect its criticality and security classification.
- documents classified as Company Restricted must have document footer on all pages and within asset registers for information processing systems.
- documents classified as Company or Client Confidential must have document footer on all pages, manual folders and in asset registers for systems processing or storage of confidential data.

Handling of assets

Moorepay has a documented Information Handling standard. The objective of the standard is to ensure the protection of its information assets, system resources and information, and to meet the legal and regulatory requirements of Moorepay, its clients and other stakeholders.

It is Moorepay's policy that appropriate control measures are implemented to protect confidential or restricted data against accidental or malicious destruction, damage, modification or disclosure and to maintain appropriate levels of confidentiality, integrity and availability of those resources. The standard outlines rules for selecting a classification for information being handled processed or stored for or on behalf of Moorepay. It supports the Information Classification Policy which mandates the requirements for protection of information.

The Standard outlines the minimum control requirement, it is the responsibility of the information owner to ensure that appropriate control measures are applied the asset.

The standard covers the rules for handling information throughout each stage of its lifecycle, including:

- labelling
- storage
- disposal
- recycling of equipment
- transit
- presentation

For each classification of data, the standard stipulates the tools and technologies authorised for use by the organisation when processing information.

The Information Handling standard applies to all Moorepay employees, vendors, partners or other interested parties who store, transmit or process information for on behalf of Moorepay.

Media handling

The following controls have been deployed to prevent unauthorised disclosure, modification, removal or destruction of information stored on media.

Management of removable media

Only authorised staff are allowed to remove items, including portable storage media, off the premises and are responsible for their safekeeping at all time.

All removable media is encrypted to standards mandated in the Moorepay Cryptography policy.

Removable media is secured adequately when not in use, in line with the controls stipulated for the classification of data contained on the media.

Removable media is securely disposed of using approved third parties to destroy the media, certificates of destruction are obtained in these circumstances. Media is stored in secure bins whilst awaiting destruction.

All laptops issued to Moorepay employees have whole disc encryption enabled.

Access and use of laptop USB drives is controlled by group policies and restricted based on the role of the user and the specific requirements.

Where USB storage devices are permitted; data encryption is enforced, ensuring that the data can only be viewed by the device used for the data copy.

Any detected use of USB ports is reported through our End User Device Management tool.

Desktop computers used in the delivery of the service have secure builds deployed that incorporate restricting access to USB drives, CD/DVD drives and local hard drives.

Disposal of media

All media used in provision of the service that is no longer of use or faulty is physically destroyed.

Destruction methods are proportional to the classification of information contained within, and as stipulated in the Moorepay Information Handling standard.

Equipment is destroyed by approved third parties, using specifically designed equipment to either shred or crush the drive.

- The hard drive shredding process shreds the entire hard drive into small pieces using industrial grade destruction equipment, and destroys the drive platters, mechanisms, and the electronic components rendering the data unrecoverable.
- Crushing is performed by punching an irreparable hole through each hard drive, destroying the drive platters, rippling and fracturing the magnetic surfaces and rendering the drive data unrecoverable.

Equipment is logged and stored securely by Moorepay prior to collection for destruction by the third party.

A chain of custody is maintained by the third party throughout the process, from collection of equipment through to issuing a certificate of destruction upon completion. Certificates of destruction are maintained by Moorepay for inspection and audit.

If required, data and software can be removed from IT storage equipment prior to destruction.

To remove Information and software before destruction, a sanitation program is used to erase disk data by writing one or more patterns to the disk, the patterns must be 1, 2, or 4 bytes long.

Confidential information on hard copy marked for destruction is stored in secure bins prior to destruction. The hard copies are destroyed by secure shredding methods by approved third parties. After shredding, the confetti-sized pieces are baled and recycled into paper products.

When paper is shredded by a supplier a certificate of disposal is issued by the third party and maintained by Moorepay for inspection and audit.

Physical media transfer

Amount of data transported using end point portable media (including laptop PCs, USB sticks; removable hard-disks and CD/DVD) are restricted. All end point portable media must be encrypted in line with Moorepay's cryptography policy.

All infrastructure-based media to be transported must be encrypted in line with Moorepay's cryptography policy.

For the transportation of media for destruction by third parties, tamper proof containers are used to transfer the equipment, barcode scanning is performed at every touch point, locked trucks and secure containers keep information secure in transit, GPS- tracked fleets are use.

Back-up media must be enclosed in a locked box and be transported by an authorised courier. The courier must sign for receipt and delivery must be recorded.

If media is transported by Moorepay employees, the media must be stored in a locked box, stowed where not on-display (such as in the locked boot of a car or secured van).

At least 2 Moorepay employees must accompany the media throughout the journey. The journey should be planned beforehand, and stops should be avoided if possible or minimized.

Identity and access management

Business requirements of access control

Moorepay has established the following controls to limit access to information and information processing facilities.

Access control policy

Access to Moorepay information and systems is governed by the Logical Access Control policy and the Physical Security policy. The policies apply to all Moorepay staff (which for this document is taken to include permanent, temporary and freelance employees and contractors) who are required to work on information and information processing assets.

Logical access control policy

The policy applies to all Moorepay's information and information processing assets, including but not limited to networks, IT infrastructure systems, applications, information storage repositories, business processes, backups, archives and information entrusted to Moorepay by its clients.

The policy covers the following areas:

- logical access principles
- logical access requirements
- banners
- password allocation
- privileged access
- segregation of duties

Physical security policy

The Moorepay Physical Security policy outlines the physical security requirements established for all Moorepay locations.

The policy covers the following area:

- physical access controls
- physical security assessments
- physical security control requirements
- access control and identification
- environmental controls

Access to networks and network services

Moorepay has deployed software agents to protect all end point devices and control access to the corporate network.

The software enables policy deployment and ensures that devices have the required prerequisite software, software updates and configuration required prior to allowing access to the network.

The software is centrally managed and integrated with Active Directory. Devices connecting to the corporate network must have the required configuration to authenticate, which along with user authentication offers pseudo Two Factor Authentication (something you have and something you know).

Access to corporate applications

Access to key corporate applications is controlled by Multi Factor Authentication (MFA) whereby the user must submit their unique username and password along with an additional “one time” authentication code.

For certain applications additional security questions are also required before access is granted.

Remote access

Remote access capability is restricted to authorised personnel only.

The same technology outlined above is used to manage remote access to Moorepay systems and information assets. Remote access is governed by the Mobile Computing and Home Working policy.

Wireless network access

Moorepay wireless networks are configured to use the WPA2 Enterprise protocol.

The connecting device must have a valid certificate installed, when the device attempts to associate to the access point, the access point queries the authentication server on behalf of the device, and only allows access if the certificate is validated.

Once a connection has been established, data transmission is encrypted using AES-CCMP standards.

Hosting environment access

Access to hosting environments is controlled by the use of multi factor authentication and is restricted to a specific group of “privileged” users.

User access management

The following controls have been deployed to ensure that authorised user have the required access and unauthorised users are prevented from accessing systems and services.

User registration and de-registration Corporate practice

All access accounts are associated with a unique user identity (User ID). The allocation of generic or shared user accounts is expressly prohibited unless authorised by the Chief Information Security Officer (CISO).

System accounts are only used where standard processes require a profile to run, these are not used or have capability to access systems.

In circumstances where temporary privileged access is required, a “break glass” process is implemented whereby authorisation must be granted and logged and access is time limited and monitored.

SaaS support services

The services have inbuilt role-based security framework and access to the application and underlying data is controlled by the customer.

- a specific “Moorepay” operator account is created, and password allocated and changed on a regular basis.
- explicit permission must be granted by the customer on each occasion that the Moorepay account is used to access the application, or,
- implicit permission is granted, whereby if a customer raises a request for assistance then it is implied that permission has been granted to access the application.

User access provisioning

All initial user provisioning requests and notification of leavers for Moorepay employees is initiated by HR via the Service Desk ticket management system. A ‘parent’ ticket is created and responsibilities of each team (e.g. networks, Infrastructure, Applications) are then advised by associated ‘sub tickets’.

By logging all activities within the Service Desk ticket management system, access administration records are maintained, providing traceability (i.e. evidence of all requests for starters, leavers and changes) of Information Asset Owner authorisation, account creation, adjustment allowing for role changes and changes to access privileges, account closure.

Management of privileged access rights

Where Moorepay employees require system level (privileged) access to the underlying system and infrastructure, appropriate and proportional access management controls are deployed.

Please see additional MAP documentation specific to your service provision for more information on privileged access management.

Management of secret authentication information of users

For new starters, passwords information is provided to the users manager on the start date and the user account is set to force the change of password on first use.

All allocated passwords are unique and align with the Moorepay Password Management standard.

Password reset request are managed by the Service Desk for corporate accounts and by the specific payroll team for Managed customers.

User identity is validated prior to changing password information.

When communicating a new password (or following a rest) to a verified user, the support team must use one of the following methods:

- via corporate instant messaging system or
- via SMS to verified mobile phone or
- verbally to verified mobile phone or
- via corporate email to a Moorepay official e-mail address

In each case the end user must be reminded to delete the message as soon as they are logged in.

Review of user access rights

User accounts are reviewed periodically to identify redundant accounts.

Corporate account user profiles are subjected to regular prescribed reviews as applicable and at least every six months to ensures that staff have been assigned the right level of privileges as per their job role and responsibilities.

Systems hosting Managed Service customers are governed by SOC1 Type II audit protocol; routine checks are performed on user profiles on a monthly basis and management reviews conducted quarterly to ensure that staff have been assigned the right level of privileges as per their function.

SaaS customers are in control of access management within their own application instance. Standard practice for the management of Moorepay accounts used to access customer applications is for the accounts to be enabled/disabled by the customer upon request and as required to deliver the contracted service. Processes are agreed between both parties and Trusted Source lists maintained to ensure that requests for access can only be submitted by named individuals.

Removal or adjustment of access rights

Leavers access to all Company systems is terminated on their last date of employment, or in the event of any suspension arising from a disciplinary procedure.

The corporate service desk system holds information regarding which systems a user has access to and has a facility to produce suitable statistics on requests.

As part of the HR leavers process, a workflow is triggered within the Moorepay service desk system that ensures all relevant parties are notified of the final date of employment of an outgoing employee. Individual child tickets are raised to ensure that all relevant access is revoked at the correct time and date.

In cases where immediate revocation of access is required, a priority ticket is raised and escalated to the appropriate team for immediate attention.

Where an employee changes role within the business, their access allocation is reviewed, appropriate access allocated based on the requirement of the new role, and access revoked where no longer require. The changes to access will be implemented within an agreed time frame that ensures continuity of service within the users old and new roles.

In cases where third parties are granted access to Moorepay systems and information, access is facilitated only for the period required and revoked immediately upon the work completing. Third parties are supervised and monitored at all times by Moorepay staff members when accessing Moorepay systems and information.

Physical security

As part of the HR leavers process, a request is raised to ensure that all access control cards are returned upon leaving the employment of Moorepay. The card will be logically disabled on the ACC system and the physical card returned to stock.

Where keys have been entrusted to an individual, they are returned before leaving the employment of Moorepay.

User responsibilities

The following controls have been deployed to ensure that Moorepay employees are accountable for safeguarding their authentication information.

Use of secret authentication information

The Password Management standard sets out the minimum technical standard for the structure and maintenance of passwords (see Password Management controls), the standard is underpinned by the Moorepay Acceptable Use of Information Systems policy which states the requirements to ensure that security controls are applied, to protect Moorepay systems that store or are used to access information.

In line with the Acceptable Use policy:

- passwords must be kept safe:
- passwords must not be written down in any manner that would make it easy to decipher and passwords must not be kept with IT equipment e.g. in a laptop bag with the laptop. This includes passwords for all information systems and websites
- any compromise of account/passwords must be reported immediately to the Security team to ensure that the appropriate actions are taken

System and application access control

The following controls have been deployed to prevent unauthorised access to systems and applications.

Information access restriction

Access to information and systems is granted strictly on a need-to-know and/or need-to-use basis, and when a legitimate business need has been demonstrated.

All access requests need to be authorised by the Information Asset Owner (IAO), or an authorised delegate of the owner. The owner must ensure that the sensitivity of those assets is known and understood so that appropriate access control rules are applied, the owner remains accountable for the proper protection of the information assets.

Access is granted only for the period required. Where access is granted to non-permanent employees (e.g. contractors, temporary employees), access must be time bound to expire on a date corresponding to the anticipated length of assignment.

Any attempt by employees to circumvent access controls or access information assets for which they are not authorised will be treated as a security incident and may be subject to disciplinary actions.

Secure log-on procedures

All access to operating systems and applications requires authentication of users, to standards stipulated in the Logical Access Management policy and Password Management Standard.

Appropriate general warning notices are displayed on systems to make users aware that unauthorised access and use of systems are prohibited, and subject to further action in case of serious security breach (e.g. disciplinary action, legal prosecution).

Account lock out after failed attempt settings are enabled to protect against brute force attack.

Information systems apply access control by design. To access information, users must have a valid username and password to gain access to any system or application.

Identities are managed through domain and system profiling; where group policies define the level of access.

Access restrictions are implemented where possible and access is limited (e.g. view, contribute, owner) according to the business requirement and in accordance with relevant legal, regulatory or contractual requirements.

Password management system

The Moorepay Password Management standard sets out the minimum technical standard for the structure and maintenance of passwords.

This standard applies to all Moorepay staff and any person working on Moorepay infrastructure (for example support company representatives).

This standard applies to all passwords used across the Moorepay infrastructure.

It is strongly advised that ‘passphrases’ are used. These are passwords made up of multiple words; either a random set or something meaningful to the user.

The Password Management standard stipulates the minimum requirements and considerations for the following areas:

- Password complexity
- passwords for standard user accounts must be at least 8 characters in length.
- should contain both letters and numbers o should contain a mixture of upper-case letters, lower case letters, numbers and special characters
- Password ageing

- passwords are not set to expire. In line with NIST best practice it is advised that passwords are only changed if suspected of compromise.
- passwords must have a minimum duration set of one day. This is to prevent users cycling passwords back to their old password (by running out the password history).
- Password history
- 12 previous passwords should be remembered and blocked from being used.
- Password lockout
- user accounts must be configured to lock after a maximum of 5 sequential invalid password entry attempts.
- accounts locked due to invalid login attempts must remain locked until re-enabled via authorised personnel.
- In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, the use of 'password manager' (vault) software is provided by Moorepay.

Use of privileged utility programs

The unauthorised use of utility programs to override or circumvent access controls is in breach of the Moorepay Logical Access Management policy and is strictly prohibited.

Where utility programs are required for support or recovery purposes, access is restricted and tightly controlled by means of a "break glass" process, whereby authorisation must be granted and logged, and access is time limited and monitored.

Cryptography Cryptographic controls

The following controls have been deployed to ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and integrity of information.

Policy on the use of cryptographic controls

Moorepay has in place a Cryptography policy, the purpose of which is to ensure that appropriate encryption control measures are implemented to protect sensitive or critical data against accidental or malicious destruction, damage, modification or disclosure and to maintain appropriate levels of confidentiality, integrity and availability of those resources.

The policy covers the following key areas of cryptography:

- general policy
- international law

- encryption of network flows
- encryption of data ‘in-transit’
- encryption of data ‘at-rest’
- management of encryption keys

The Cryptography General policy stipulates that:

- The use of cryptography must be commensurate with the value and sensitivity of the information concerned, and the risks to which it is exposed.
- Procedures must be established to ensure the availability of encrypted information in the event of loss of an encryption key.
- The use of cryptographic controls must be consistent with all relevant legal and regulatory requirements.
- Acceptable key strengths and algorithms must be defined by the Security team and reviewed on a regular basis.
- All licenses must be obtained to export, import and/or use products containing cryptography.
- All keys must be protected by physical and logical controls to ensure they are not compromised
- There must be an approved and documented key management process for managing the full lifecycle of cryptographic keys within Moorepay.
- Encryption must be implemented whenever communicating client or personally identifiable information (PII) outside of the organisation.
- All passwords must be communicated over a different medium than the encrypted (protected) information.
- Any internet facing service requiring public key infrastructure (PKI) must use certificates signed by a certificate authority (CA) approved by the Security team.
- All laptops must be encrypted using whole-disk encryption.
- All Mobile devices must be encrypted using Company mobile encryption protocols.

The policy is supported by the Moorepay Information Handling standard which outlines the rules to be applied when handling, storing and processing information.

Key management

The Moorepay Cryptography policy stipulates the following regarding key management:

- encryption keys must be managed in such a way that ensures encrypted stored data will neither become unrecoverable nor accessible by an unauthorised person

- ensure that master encryption keys are stored in a secure location, and appropriately protected from environmental and accidental damage.
- ensure that encryption keys are not held within a database that is encrypted with those keys or on the same host
- record who holds the encryption keys (key custodians) required to decrypt important information
- revoke or change encryption when key holders leave.
- where technically enforceable, the strongest encryption (including key length) and hashing algorithms must be deployed.
- certificates must be signed by a known, trusted provider.

Physical and environmental security

Physical security policies

Moorepay has in place the following polices and standards to ensure that all locations that host its critical IT facilities, services and information, are protected from unauthorised physical access, environmental threats and other threats that have a material impact on security of the information.

Physical Security policy

This document outlines the physical security requirements established by Moorepay for all Moorepay locations. Any deviation from the established requirements needs to be approved by Corporate Real Estate and Security.

Data Centre Security standard

This document lays down the standards required to protect Data centres and on-site IT equipment/server rooms protecting Moorepay's primary IT resources from a range of physical and environmental threats.

Data centre security

Data centres used for Moorepay private cloud and public cloud offerings are provided by established third party data centre providers.

Robust assurance checks are completed to ensure that the data centre provider aligns with Moorepay security requirements and data centres are subject to regular auditing to ensure ongoing compliance.

Please see additional MAP documentation specific to your service provision for more information on data centre physical security controls.

Secure areas

The following controls have been deployed as standard across Moorepay Service Centres and other locations to prevent unauthorised physical access, damage and interference to Moorepay 's information and information processing facilities.

Physical entry controls

The physical premises of all buildings used by Moorepay and its subsidiaries is secured by appropriate and reasonable means. Access is denied to those who do not have a

legitimate business need to enter the site. All premises and equivalent follow basic policies and best practices to ensure the best possible physical security based on the criticality of the assets to protect and the level of risk.

The minimum safeguards authorised are;

- Physical access controls (access badges): to avoid non Moorepay persons to enter premises and;
- Identity control (id badges): to allow control of person who enter Moorepay premises.

Employees are not permitted to share badges or grant access to the site to any fellow employee (this includes following another employee into the building after the prior employee swipes theirbadge i.e. piggybacking).

Each employee is tasked with making sure their building is secure by following the guidelines outlined in the Moorepay Physical Security policy.

Visitors to Moorepay Service Centres must only be granted access on invitation by Moorepay in advance, where possible, or, where there is a requirement for unplanned visitors (e.g. emergency access), a Moorepay host must be available to meet the visitor and oversee their activities while they are in attendance.

All visitors to Moorepay Service Centres must always sign in upon entry, the following information is recorded in the visitor’s log:

- Full name
- Signature

- Time of arrival
- Time of departure
- Contact at site

Securing offices, rooms and facilities

Information and Information processing facilities are stored in a secure area preventing unauthorised access.

A combination of card, PIN and 'mechanical push locks' is used to control entry to secure areas.

Pass codes are known only to the staff authorised to enter those facilities.

Protecting against external and environmental threats

Suitable suppression, detection and alerting systems are in place to protect the assets against environmental threats.

Working in secure areas

Local divisions and departments are responsible for creating appropriate procedures and work instructions for working in secure areas. Controls are implemented based on the sensitivity of information processed, all legal, regulatory and contractual requirements, and in line with Moorepay Security and Privacy policies. Controls may include but are not limited to the following:

- screen protection and/or obscure windows
- prohibited use and possession of mobile devices
- CCTV at entrances and within processing areas.
- secure builds preventing the ability to save or transfer data locally

Access to secure areas is granted on a "need to use" basis where business justification has been submitted and access approved.

Appropriate guidance notices are issued to staff required to work in secure areas.

Delivery and loading areas

Appropriate physical security controls are deployed to ensure that public access, delivery and loading areas are isolated from information processing facilities.

- entrances to loading areas are secured in line with the Moorepay Physical Security policy.
- designated personnel are assigned to monitor and control access via loading areas.
- personnel using loading and delivery areas are monitored both physically and by CCTV at all times.
- where applicable, routes between delivery and loading areas and operational facilities have physical security controls deployed.

Equipment

The following controls have been deployed to prevent loss, damage, theft or compromise of assets and interruption to Moorepay's operations.

Equipment siting and protection

Information systems are sited in fit for purpose server rooms.

A combination of card, PIN and 'mechanical push locks' is used to control entry to the server rooms. Pass codes are known only to the staff authorised to enter those facilities.

Server, storage and network equipment is housed within server racks that are secured at all sides to prevent equipment tampering and access to ports and drives.

Supporting utilities

The following controls are deployed as standard to protect applicable equipment:

- flood and Fire detection and suppression systems
- UPS and power generators
- heat regulation (air conditioning + heat sensors)

Maintenance agreements are in place and regular equipment tests undertaken to ensure the effectiveness of the supporting controls.

Audits are undertaken at least annually by Moorepay to ensure that the correct equipment is in place and maintained effectively.

Equipment maintenance

Moorepay has appropriate back-to-back contracts and Service Level Agreements in place with the relevant third parties.

Equipment is maintained in line with vendors recommendations.

Where third parties are engaged, appropriate monitoring of activity is maintained.

Repaired equipment is thoroughly tested prior to reintroduction into production environments.

Removal of assets

Assets issued to end users are signed for by the user and record kept against the asset entry within the corporate ticketing system.

Software is installed by authorised support personnel and retained within secure libraries.

Assets cannot be removed from the data centre without prior approval from the site management.

Any equipment removed from a data centre or service centre is recorded as being moved offsite and recorded when returned.

Security of equipment and assets off-premise

Moorepay has a Mobile Computing and Home Working Security policy that covers the security of mobile devices.

This Policy applies to all employees and third parties working remotely or using mobile devices (which for this document are taken to mean mobile phones, tablets, laptops, macs or other easily transportable computing equipment) who are provided with authorised access to information and information processing systems.

All employees and authorised third parties must comply with this Policy.

- mobile devices that are supplied and supported by Moorepay are permitted to connect to and access information on the networks. All such devices must have the corporate management tools installed to enable them to be remotely managed and data wiped if necessary.
- all mobile devices must have disc encryption enforced.
- all mobile devices must be password or pin code protected.
- laptops must be supplied and supported by Moorepay. User owned devices are explicitly forbidden to be connected to networks or information assets. Special dispensation can be applied through exception, only where a specific business justification and approval is in place.

- in order to provide strong protection against unauthorised information access in the case of loss, laptops must be protected with approved encryption software. Passwords must comply with the Moorepay User Password Policy.
- all laptops must have anti-malware software installed by default and employees must ensure that this is regularly updated on their device. Mobiles and Tablets should have anti-malware installed (including personal devices).

Employees must:

- keep mobile devices in their possession and within line of sight whenever possible.
- take extreme care to protect confidentiality and minimise risk of exposure by limiting information that can be seen by others.
- store mobile devices out of sight when not in use.
- take mobile devices home with them outside office hours.
- keep phone conversations discreet and avoid being overheard, turn off the Bluetooth facility when not essential and/or set to “hidden” to avoid calls being intercepted.
- transport laptops and tablets out of sight when carried in a car, preferably in a locked boot.

Employees must not permit any unauthorised user to access a Moorepay device or permit access to Moorepay data or networks from a user owned device that is authorised for business use, this includes family members.

In the event of a mobile device being lost or stolen, IT Services must be informed immediately to ensure the account is disabled and data wiped.

Secure disposal or re-use of equipment

All media used in provision of the service that is no longer of use or faulty is physically destroyed.

Equipment is logged and stored securely by Moorepay prior to collection for destruction by the third party.

To remove Information and software before destruction, a sanitation program is used. Certificates of destruction are maintained by Moorepay for inspection and audit.

Unattended user equipment

All user workstations are locked when left unattended.

Group policy ensures that all end user systems processing customer data are automatically locked after a defined period of inactivity. User re-authentication is required to regain access to the system following lock out.

Clear desk and clear screen policy

The Moorepay Clear Desk – Clear Screen policy establishes the requirements for employees to ensure that protection of confidential information is maintained when electronic files and documents are in their possession:

This Policy applies to all Moorepay employees and third parties provided with authorised access to Moorepay's premises, information and information processing

equipment or facilities, including data, communications or telephony networks, cloud applications, static and mobile computing devices and associated removable media.

All managers are responsible for implementing the Clear Desk/Clear Screen policy within their areas of responsibility. All employees must comply with this Clear Desk/Clear Screen policy.

- outside working hours, desks must be cleared of all confidential documented information, whether protectively marked or not.
- whenever a desk is left unattended, confidential documented information must be secured in appropriate lockable storage.
- screen locking facilities must be used when leaving a desktop computer or portable device unattended to prevent unauthorised viewing of confidential information.
- outside working hours, all desktop and laptop computers must be turned off, unless they are required to remain on for operational purposes. All devices that are left switched on must be logged out.
- all information classified as Company confidential or Company restricted must be disposed of in a secure manner as stipulated in the Standard for Handling Information.
- documents must be removed promptly from printers, photocopiers and fax machines.
- outside working hours, unopened mail must be locked away.
- outside working hours, laptop computers, mobile telephones and other portable assets and keys must be locked away.
- those in charge of meetings must ensure that no confidential information is left in the room, either on the table, slides, flip charts or boards when the room is not occupied

Locked offices and restricted areas do not provide exemption from this Clear Desk/Clear Screen policy.

Operations security

Operational procedures and responsibilities

The following controls have been deployed to ensure the correct and secure operations of information processing facilities.

Documented operating procedures

Business divisions and local departments are responsible for creating appropriate work instructions and procedures to align with the corporate policies and standards.

Where processing of data is involved, Standard Operating Procedures (SOP's) are maintained that ensure each operative fully understands the process steps that must

be followed. SOP's incorporate validation steps to ensure integrity and confidentiality of data.

Extensive documentation is maintained which includes but is not limited to the following:

- build and deployment documentation
- system diagrams and data flows
- security processes and guides
- ITIL processes

Change management

To ensure that there is no negative impact on business operations or information security, formal Change management responsibilities and procedures have been implemented to control all changes to information systems.

When changes are made, as a minimum, the following is covered in the change process:

- identification and recording of the change
- planning and testing of the change
- assessment of the potential security impacts of the change, in line with

Moorepay Information Security Risk Management policies and procedures

- formal approval for the proposed change
- communication of the change details to all relevant people
- fall-back procedures, including procedures and responsibilities for aborting and recovering from an unsuccessful change and/or unforeseen events.

Moorepay client account managers and service owners are responsible for

communicating changes to clients where the change will impact on the confidentiality, integrity or availability of client data.

Risk assessment

Risk assessments are conducted when required by the Security team prior to approving change.

Projects that aim to handle Confidential or Restricted information are subject to a Data Privacy Impact Assessment (DPIA).

Emergency change

In circumstances where a change is required as part of remediation activities due to a severity 1 or severity 2 level incident, the emergency change process can be initiated to ensure the timely resolution of the incident.

The emergency change process requires that an Emergency Change Approval Board (ECAB) is convened to review the change details and process the change efficiently. As a minimum the following is covered in the emergency change process:

- identification and recording of the change
- planning and testing of the change
- assessment of the potential security impacts of the change, in line with UKI Information Security Risk Management policies and procedures

The technical teams and/or change task implementer must be present at the E-CAB meeting and be able to speak on behalf of the change status and technical criteria.

Approval to proceed can be given by the E-CAB if the above criteria is met.

Capacity management

Systems are architected to ensure additional capacity is always available to cope with unexpected and planned peaks in processing.

Capacity demands are monitored, and projections of future capacity requirements made.

The system components included in scope when reviewing the current state of the environment capacity are CPU, memory, storage and host network performance across production system environments. There are different tools sets gathering this

information daily, providing different information points of each environment component which contribute to providing an overall capacity summary of an environment.

The multiple data sources are collated to build a report of the usage pattern of the infrastructure.

Separation of development, testing and operational environments

Development, test and operational facilities are physically and logically separated. Development is carried out on specific servers that are not part of the production hosting infrastructure.

Changes are carried out in test environments for both application and infrastructure before being promoted into production.

The implementation of changes in the production environment is done under strict change control.

Protection from malware

The following controls have been deployed to ensure that information and information processing facilities are protected against malware.

Controls against malware

Market leading anti-malware software is installed on all Moorepay desktop computers, laptops and applicable servers used to provide the service.

Personal firewalls are enabled on all end points.

Employees are not permitted to remove or deactivate anti-virus scanning software or personal firewalls.

In addition:

- traffic inspection devices and traffic inspection analyser devices are deployed across Moorepay network environments to analyse incoming and outgoing traffic and to detect and quarantine suspicious content.
- all incoming emails are scanned for malicious code using a separate product suite.
- white listing is in place to ensure that access is restricted to approved internet sites and services where there is a legitimate business need.

Moorepay employees are provided with awareness training and techniques to identify malicious activity and to avoid propagating virus's and malware or falling victim to malicious attack.

Any malware or phishing issue must be reported as a security incident (whether real or suspected) following the guidance in the Moorepay Security Incident Management policy.

Backups

Moorepay has implemented suitable data backup solutions across its platforms to protect against loss of data and to ensure data recovery in line with contractual requirements.

Please see additional MAP documentation specific to your service provision for more information on data backups

Logging and monitoring

Appropriate logging is enabled on all servers and network devices in line with the Moorepay Operational Security policy to ensure that important security-related events are:

- recorded in logs
- stored and protected against unauthorised change or access
- securely transmitted to appropriate log management analysers
- reviewed and analysed on a regular basis; and
- kept for an appropriate period

Please see additional MAP documentation specific to your service provision for more information on logging and monitoring.

Log retention

Logs are archived prior to deletion and retained for a minimum of 12 months.

Security Information and Event Management

Moorepay has in place a Security Information and Event Management (SIEM) system.

Logs from servers, network devices and database are copied to the SIEM and analysed by qualified Security Operations Centre (SOC) personnel for abnormal activity that may represent an Indicator of Compromise (IoC).

Alerts are correlated and investigated by the SOC to determine if they are genuine IoC's. Documented response plans are in place to ensure the timely escalation and response to IoC's.

The SOC operate on a 24/7/365 basis.

SIEM logs are retained for 60 days by default.

Administrator and operator logs

To ensure that logs that record privileged user account activity are protected and reviewed to ensure that privileged account holders are not manipulating the logs on information processing facilities under their direct control, the logs are copied to the SIEM system for analysis.

There is a Segregation of Duties policy enforced that ensures that System Administrators do not have access to the SIEM system.

Clock synchronisation

All appropriate clocks are synchronised using an NTP service or equivalent and align to a single source. This covers both operating systems and applications where the accurate timings are required for non-repudiation issues.

Control of operational software

The following controls ensure the integrity of operational systems.

Installation of software on operational systems

All software installations must follow the standard change management process and as such undergo the required authorisation, review and approval steps prior to installation.

Software is deployed in a QA environment and fully tested prior to deployment into production.

For new software acquisitions, the supplier must undergo the requisite checks in line with the Moorepay Supplier Assurance process beforehand.

Depending on the nature of the software and the potential impact on the security of data, further solution assessments may be undertaken by the Security team and approval required before deployment.

For major software acquisitions and changes, the Technical Advisory Board (TAB) is engaged to fully assess and approve the acquisition.

Technical vulnerability management

The following controls have been deployed to prevent the exploitation of technical vulnerabilities.

Management of technical vulnerabilities

Moorepay has a Vulnerability Management standard that establishes the minimum requirements to be deployed for a sound vulnerability discovery and management system.

The standard covers the following key areas of vulnerability management:

- patch management
- penetration testing
- vulnerability scanning

The standard includes requirements for vulnerability discovery and response.

In addition to the above, Moorepay maintains a Standard for Patch Management which aims to define a common management framework in applying patches on production systems to reduce risks, resulting from exploitation of technical vulnerabilities, in an effective, systematic, and repeatable way.

The standard covers the following types of patches:

- security patch
- hot-fix
- service pack
- software update

The Moorepay Patch Management standard applies to all computing devices that are susceptible to vulnerabilities, including:

- network routers and switches
- servers
- desktops
- laptops
- mobile devices
- associated software/firmware applications within the Moorepay technology landscape.

Moorepay patch management practice

Information regarding patches and updates are received from reliable sources and system health check analysis is performed daily.

The timeframe to deploy patches is dependent on many factors, including the criticality of the patch, the criticality of the system requiring the patch, service downtime and its impact to customers.

- Critical patches are deployed in the production environment within 14 days of release.
- High priority patches are deployed in the production environment within 14 days of release.
- All other applicable Windows patches are deployed within 30 days of the patch being agreed.
- Additional patches within the hosting environment are deployed at least twice yearly

Patch deployment

Patches are installed in a test environment prior to installation in the production environment.

Where possible patches are installed into production during pre-agreed maintenance windows when downtime is required.

The process for the deployment of patches within the production environment is as follows:

- identifying vulnerabilities and patches
- information regarding security patches and updates are received from reliable sources and system health check analysis is performed daily. Security testing is carried out regularly to highlight exposure to known vulnerabilities.

- general patch information is reviewed regularly, and patches applied when there is a specific requirement, i.e. New functionality is deemed to be of benefit, or support schedules enforce an update.
- standard contractual terms determine the release schedule for core applications.
- patch validation and testing.
- the patch file is validated, to ensure that it has not been altered while in transit.
- the validated patch file is virus checked, where applicable, using up-to- date virus scanning software in an isolated and a safe network location.
- patch deployment testing is carried out on a “test” system that represents the production system as closely as possible, to assure that it addresses the vulnerability it purports to fix, and the introduction of new patches does not break or alter system functionality needed by business-critical applications or services.
- deploying patches
- a suitable backup of the systems is completed, where possible, prior to installing the patch in the production environment.
- a change request is raised and approved before applying the patch on production systems and applications
- post-patch functionality testing is performed, where applicable, to ascertain the patch has been deployed as intended and the vulnerability has been eliminated successfully.
- the asset inventory and/or the Baseline Configuration document is updated to reflect the newly installed patch detail.

Moorepay penetration testing practice

Moorepay contracts with independent third parties to conduct the following:

- twice yearly infrastructure penetration tests, and
- pre-release application penetration tests

The aim of infrastructure penetration testing is to ensure that the infrastructure supporting any public facing services is not susceptible to attack from known vulnerabilities and threats. Testing is conducted against the applicable public interfaces within the production environment.

Application penetration testing forms part of the application development processes adopted by Moorepay software development teams to ensure that vulnerabilities are identified and remediated in new product releases.

Application penetration testing is conducted in the QA environment. The QA environment mirrors the production environment in terms of platform, infrastructure and perimeter security.

The overall methodology adopted by the contracted penetration testers is based on the best practice of the OpenSource Security Testing Methodology Manual (OSSTMM) which defines an internationally recognised set of rules, guidelines and approach to security testing and security assessment of an organisation.

Testing is non-intrusive and involves no intentional exploitation of vulnerabilities beyond that necessary to demonstrate the vulnerabilities exist, unless specifically requested beforehand.

The penetration testing process is broadly broken down into the phases summarised as follows:

- foot-printing (research)
- basic intelligence is gathered on the Internet to obtain corporate information about network addresses, IT deployment, and network topology.
- enumeration
- scanning of the systems is conducted to identify open ports, services and architectural features. Automated scanning is utilised, and the raw data generated is interpreted by a security specialist.
- exploitation
- methods employed by hackers is simulated in that the data gathered during enumeration is used to plan the next steps in penetrate and exploit the target systems.
- analysis
- findings are examined, correlated with best practice and current knowledge bases, and vulnerabilities prioritised.
- reporting
- report are produced highlighting analysed risk areas.

Moorepay vulnerability scanning practice

Both internal and external vulnerability scanning is performed on a monthly basis. Internal scanning is performed by qualified Moorepay personnel.

External Vulnerability scanning is performed by a qualified third parties. The scanning is conducted against all externally facing infrastructure.

The vulnerability assessment is based on proven proprietary technology created to provide an accurate scanning service while still maintaining network availability.

The vulnerability database is routinely updated with the latest vulnerabilities and is aligned with the CVE (Common Vulnerability and Exposures) standard for information security vulnerability names.

The managed vulnerability assessments are performed in accordance with the following assessment methodology:

- verification
- conducted on the first scan only for each IP address, focused on checks associated with verification, in place to ensure input data errors do not propagate into further stages of the assessment and assure the integrity of the scanning operations.
- service scanning
- the service scanning phase of the assessment identifies all responding TCP, UDP and ICMP services.
- service enumeration
- once the presence of a service has been confirmed, banner information capture is attempted to assist in determining machine vulnerability status.
- vulnerability detection
- this phase consists of performing a configurable number of tests, from a range of application layer vulnerability tests down to a single specific test if necessary, against those services discovered in earlier phases of the assessment. A large number of separate tests are performed; tools are continually updated with the latest vulnerability exploits.
- reporting
- reporting contains the findings together with corrective actions, historical trends and summary statistics.

Output from the scanning is provided to Moorepay for further processing, all vulnerabilities are logged within the Moorepay ticketing system and remediated according to priority by qualified Moorepay personnel.

Summary reports are not currently part of the standard service offering and are not available for distribution externally.

Vulnerability remediation

For each vulnerability detected, a Common Vulnerability Scoring System (CVSS) score is allocated (based on a 1 to 10 range). This score is used along with other determining factors to grade each detected vulnerability.

The risk assessment levels assigned are based on the following definitions:

- critical

the vulnerability either critically exposes the client to risk of compromise or possibly there is a high likelihood of it having been compromised already owing to it being widely known and simply exploited.

- high

an issue which, if exploited, has the potential for severe impact on the confidentiality, availability and/or integrity of your information assets; the issue may be relatively straightforward to uncover or technical exploitation of this may be relatively trivial.

- medium

an issue which, if exploited, has the potential for a moderate level of impact on the confidentiality, availability and/or integrity of your information assets;

discovery of the issue may require a reasonable level of technical capability and it may also be technically quite challenging to exploit or require a reasonable level of resource/time.

- low

an issue which, if exploited, has a potentially low level of impact on the confidentiality, availability and/or integrity of your information assets; it may also be technically difficult to exploit in reality or require significant resource/time allocation.

All vulnerabilities identified are subject to remediation and tracked through their lifecycle. Critical, high and medium vulnerabilities are addressed as a matter of priority, low and informational vulnerabilities are recorded and highlighted for future

consideration. In the case of applications this might require an isolated security patch delivered once a new release is already in production. All remediation actions follow internal standard deployment procedure under strict change control.

Standard Moorepay global service desk parameters are applied for response and remediation of vulnerabilities as follows:

- critical – within 14 days of discovery
- high – within 14 days of discovery
- medium – within 6 months of the vulnerability being reported.
- low – within 12 months of the vulnerability being reported.

Timeframes for remediation of detected vulnerabilities is dictated primarily by severity and impact as outlined above. However, the complexity and impact to services of the remediation activities may also be taken into consideration and in certain circumstances, delays may be agreed, and short term risks accepted where remediation is focused on longer term projects.

Restrictions on software installation

All software installations must follow the standard change management process and as such undergo the required authorisation, review and approval steps prior to installation.

Standard builds are deployed to desktop and laptop computers that include removal of administrator rights and the ability to install software.

A list of approved software is maintained and accessible from each end user computer. via the Moorepay Software Centre.

Requests for software are submitted via the Software Centre, a request is then raised within the Moorepay Service Management system and management approval confirmed following assessment before proceeding with the installation.

Further controls on the installation and use of software are contained within the Moorepay Acceptable Use of Information Systems policy.

Failure to align with policies can result in disciplinary proceedings.

Information systems audit considerations

The following controls have been deployed to minimise the impact of audit activities on operational systems.

Information systems audit controls

Specific control test (automated and manual) are conducted on a regular basis and the results recorded for audit purposes.

The tests are designed to give assurances that specific technical and operational controls are effective and operating within agreed boundaries.

Tests are designed to ensure there is no negative impact on the confidentiality, integrity and availability of information.

Audits are planned and conducted with consideration given to operational requirements and with the agreement of senior leaders and asset owners.

Communications security

Network security management

The following controls have been deployed to ensure that information in networks and supporting information processing facilities are protected.

Please see additional MAP documentation specific to your service provision for more information on network security.

Network controls Moorepay has in place the following policies and standards to ensure that all networks and relevant components are configured securely and managed appropriately to protect the confidentiality, integrity and availability of Moorepay and its customers information:

- Network Security policy
- Firewall Management policy
- Firewall Management standard

Moorepay has a Network Operations team responsible for and dedicated to the management of the Moorepay environments, including corporate LAN and WAN, hosting environment, and wireless networks.

Access to network and firewall devices is restricted to specific management IP.

addresses located on the internal “trusted” network. HTTPS and SSH are the secure encrypted protocols used for management access.

Firewalls are deployed at each network boundary, all IP traffic entering or leaving a Moorepay network must traverse the firewall. In line with firewall management best practice, the following is implemented as standard.

- by default, firewalls must operate under an implicit deny and prevent any traffic from flowing inwards or outwards unless that traffic has been specifically approved via change control.

- firewalls must never fail open, such that they allow traffic to pass freely in the event of a device failure. Any failure must result in zero throughput (fail Secure).
- all perimeter systems must be securely configured (hardened).

When individual changes are carried out to firewalls, rulesets are reviewed to ensure there are no security issues caused by the change, and to remove any redundant rules that may have been created.

Segregation in networks

As standard, the following architectural principles are deployed:

- traffic is prevented from flowing directly between applications and external networks (internet) by the implementation of DMZ hosted firewalls.
- firewalls are deployed between corporate networks and the customer hosting environments.
- firewalls are deployed to segregate customer environments.

Information transfer

The following controls have been deployed to maintain the security of information transferred within Moorepay and with any external entity.

Information transfer policies and procedures

Moorepay Information Classification and Ownership policy outlines rules for selecting a classification for information being handled processed or stored for or on behalf of Moorepay. Supporting this is the Information Handling standard which mandates the requirements for protection of information to meet legal, contractual and business requirements.

Agreements are drawn up for the transfer of data between Moorepay and its customers, as standard the following methods are allowed and aligned to the Data Handling standard and Cryptographic policy:

- data transfer between the data centres and client PC's are secured using HTTPS and digital certificates.
- interface file transfer is provisioned via an SFTP Portal that uses unique credentials per customer.
- HTTPS, SFTP and FTPS protocols use SSL/TLS/SSH encryption algorithms with a 256 key length where the target systems allow.

Data transfer between Moorepay and its third parties is agreed and addressed via contracts, statement of work and strategic partnership agreement.

Data Protection Impact Assessments (DPIA's) are completed and data flow diagrams drawn up to fully understand the flow of data, the associated risk points to enable secure transfer solutions to be implemented.

Agreements on information transfer

Moorepay has appropriate back-to-back contracts and Service Level Agreements in place with the relevant third parties.

Security requirements are addressed via contracts, statement of work and strategic partnership agreement.

Standard contracts stipulate that suppliers must comply with laws and regulations regarding data privacy and data protection, including but not limited to the Data Protection Act 2018.

It is mandated that suppliers must comply with Moorepay's Abridged Data Privacy policy and Security and Compliance standard for Outsourced Third Party Service.

Providers and must implement and maintain appropriate technical and organisational measures and other protections for personal data.

Electronic messaging

The Moorepay corporate email system is configured to use speculative TLS for outbound emails whereby if the receiving system has TLS capability, then TLS is used to encrypt the information in transit.

The Moorepay Information Handling standard stipulates that, confidential information must be encrypted when transferring using email, unless agreed in writing with the client.

All incoming emails are scanned for malicious code.

Access to webmail is prohibited and whitelisting is in place to ensure that access is restricted to approved internet sites and services where there is a legitimate business need.

Confidentiality or non-disclosure agreements

Confidentiality agreements are included in standard employee contracts of employment and stipulate that employees maintain the confidentiality of the Company's information, do not discuss the Company's affairs in public places or disclose confidential information outside the Company without authority.

Failure to observe the above would result in disciplinary action and any breach of confidentiality may be considered as gross misconduct.

Confidentiality clauses are included in standard Terms & Conditions in place with suppliers, and stipulate that suppliers will hold in confidence, use only for the purpose of providing Moorepay products or services and avoid disclosure to any third party all Moorepay confidential Information.

"Moorepay confidential information" shall include all non-public information which Moorepay provides to suppliers under the agreement, or which is obtained or created by the supplier while providing the products or services, and that, the supplier will employ appropriate security procedures to ensure the non-disclosure of Moorepay confidential information.

System acquisition, development and maintenance Security requirements of information systems

The following controls have been deployed to ensure that information security is an integral part of information systems across the entire lifecycle.

Information security requirements analysis and specification

The Technical Advisory Board (TAB) validates proposals for new technology.

The Change Advisory Board (CAB) validates proposals for major changes to existing systems.

The Security team involvement in the TAB and CAB processes ensures:

- the incorporation of security and privacy controls into proposed solution compliance with security and privacy policies
- satisfactory completion of data security and privacy assessment as evidence of compliance with security and privacy requirements.

Securing application services on public networks

Public (internet) facing applications are secured in line with the Moorepay Information Handling standard and Cryptography policy.

Methods of connection and data transfer are included in customer service agreements, supplier contracts and strategic partnership agreement.

Protecting application services transactions

Secure point to point connections are maintained between service and client.

Suitable encryption technologies are deployed for information in transit, in line with Moorepay Information Handling standard and Cryptography policies.

Digital certificates are secured in line with Moorepay key management standards. Application validation rules provide data integrity.

Security in development and support processes

The following controls have been deployed to ensure that information security is designed and implemented within the development lifecycle of information systems.

Secure development policy

The Moorepay Secure Development policy applies to the acquisition, development and maintenance of all software, systems, equipment and services which support Moorepay information assets.

All of Moorepay IT system development activities and suppliers providing information systems and services to Moorepay are required to comply with this policy.

The objectives of secure application development are:

- to build information security into the entire lifecycle of application acquisition, development and maintenance.
- to make sure that when information systems are designed and implemented, information security is an integral part of the lifecycle.
- to build appropriate levels of protection of data used for testing information systems.

The policy covers the following principles of development, acquisition and maintenance that should be followed as standard:

- security requirements, analysis and specification

- secure coding standards
- correct processing in applications
- control of operational software
- software suppliers
- outsourced development
- protection of test data
- access to program source code
- deployment of applications

System change control procedures

Infrastructure and system changes are managed and controlled by the operational change management process outlined previously in this document.

Technical review of applications after operating platform changes

Changes to the operating platforms are tested in a secure QA environment prior to release into production.

Bespoke test scripts are developed, and acceptance criteria defined to ensure that issues are identified and resolved and the potential for adverse impact is removed prior to implementing changes into production environments.

Restrictions on changes to software packages

Modifications to vendor supplied software is not general practice within Moorepay. Where modifications are required, standard practice is to ensure that there is no impact on the service and support agreements in place.

All modifications to software packages (internally developed or acquired) are carried out in line with the change management process and fully tested in a QA environment before deployment into production.

Secure system engineering principles

Moorepay has a Secure Server Build standard that provides the fundamental principles that form the basis for a standard build architecture and ensures repeatable and consistent builds are deployed across the entire server estate. The standard focuses on the principles and objectives that form the Operating System component of a server build referred to as the Standard Operating Environment (SOE).

The SOE build applies to physical or virtual servers built for use by Moorepay. The Secure Build standard cover in detail the following key requirements:

- operating system configuration
- operating system hardening, including but not limited to,
- disabling of unrequired protocols, services and ports
- removal of development and management tools
- removal or renaming of default accounts and passwords
- disc encryption
- identity and access management
- patching
- logging
- security services, including but not limited to,
- anti-malware configuration and management
- registration with vulnerability scanning service
- registration with SIEM
- registration with patch management policy
- backup

Secure development environment

Development, test and operational facilities are physically and logically separated.

Development is carried out on specific servers that are not part of the production hosting infrastructure. Access to development and test environments is controlled in accordance with the Moorepay Logical Access Management policy.

Outsourced development

Systems used in the delivery of the services are owned and maintained by Moorepay. All intellectual property (IP) is owned and controlled by Moorepay.

Only Moorepay preferred suppliers are used for the provision of outsourced development resource.

All resources must abide by and align with all corporate security, compliance and HR policies.

Where professional services are used in implementation of new technologies, supervision and monitoring is mandated.

System security testing

Information on internal review and testing procedures, including test scripts, acceptance criteria, stories development, etc.

Moorepay hosted applications are all penetration tested, at least annually or each major release of software, based on tests recommended by OWASP, The Open Web Application Security Project .

Penetration testing is conducted by independent, qualified third parties.

System acceptance testing

Builds are compiled, and full test automation runs (and passes) before a build can be made available in a formal QA environment. Following QA sign-off, builds are then made available for production release or scheduled monthly patch releases and can only then be promoted to Test and Live.

Weekly shiproom to discuss the content and progress of the next SMR release are held to discuss the content of the release.

Protection of test data

Real data is not used outside of the production environments without explicit instruction from the data controller.

Supplier relationships

Information security in supplier relationships

The following controls have been deployed to ensure the protection of Moorepay's assets that are accessible by suppliers.

Information security policy for supplier relationships

The Moorepay Supplier Security policy mandates the Company's requirement for appropriate security in supplier relationships. Moorepay recognises that to provide services to its stakeholders (customers, employees, etc) it may need to engage the products and services of a third party (and their suppliers).

These requirements are aimed at protecting the confidentiality, integrity and availability of information handled, stored and/or processed by approved suppliers (and their suppliers).

All those acting on behalf of Moorepay must adhere to the Supplier Security policy when suppliers' will access, or potentially will access Moorepay or its customers information.

The Procurement team performs a strict set of evaluation steps in the sourcing and on-boarding of potential suppliers. The life cycle of sourcing includes the following major steps.

- inventorying potential suppliers for the target supplier categories, i.e. sourcing suppliers with the right service offering and compliance make-up required.
- engaging with the inventoried candidate suppliers to discuss the objective of services.
- completing Non-Disclosure Agreements.
- presenting the supplier engagement model to the potential suppliers.
- managing supplier through the evaluation process.

Moorepay supplier evaluation model varies based on the risk level of suppliers with varying degrees of analysis depending on the nature and sensitivity of services being provided.

The Security team are engaged by Procurement for the sourcing, selection and on-boarding of any new suppliers. This is done as soon as the need for a supplier is recognised by the Business.

All Suppliers undergo an initial security and privacy risk assessment ahead of any contract completion. Security and privacy risk assessments include corporate compliance checks and an assessment of the supplier's available certifications and assurance documentation.

Moorepay risk-based due diligence approach devotes attention and resources to those relationships that pose the most significant risks. While all suppliers are subject to security and compliance due diligence and supplier assurance program, security assessment of suppliers is conducted in accordance with a risk-based approach, with potential on-site audits occurring for high-risk partners.

The approach considers various risk factors, such as:

- the country of operation
- the business opportunity
- the type of Supplier relationship
- the size of the business relationship and

- the potential level of interaction with Moorepay and/or customer information within the categories set out in the Information Handling and Ownership policy.

Addressing security within supplier agreements

Security requirements are addressed via contracts, statement of work and strategic partnership agreement.

Standard contracts stipulate that suppliers must comply with laws and regulations regarding data privacy and data protection, including but not limited to the GDPR / Data Protection Act 2018.

It is mandated that suppliers must comply with Moorepay's Abridged Data Privacy policy and Security and Compliance standard for Outsourced Third Party Service

Providers and must implement and maintain appropriate technical and organisational measures and other protections for personal data, in areas including but not limited to the following:

- risk management
- user awareness
- incident and change management
- user access
- data protection
- physical security
- business continuity and disaster recovery
- cryptography
- vulnerability management

Information and communication technology supply chain

Risks associated with information and communication technologies are considered as part of supplier risk assessment. Where applicable, more in-depth review of these elements of the service are undertaken, and appropriate risk control agreed with the supplier.

Supplier service delivery management

The following controls have been deployed to maintain an agreed level of information security and service delivery in line with supplier agreements.

Monitoring and review of supplier services

Suppliers are re-evaluated periodically for compliance with Moorepay requirements.

The frequency of this review is determined by the classification of the supplier and may be increased or decreased depending on the risk assessment of any security and/or compliance findings encountered during a given evaluation period, including but not limited to; any serious or repeated security and/or compliance incidents which indicate a compliance system failure, or are any major organisational changes.

Potential disengagement is considered where there are any serious and/or repeated findings.

Suppliers are assessed by qualified personnel who examine the policies, processes and procedures supplied by the supplier.

Assessments are reviewed for follow-up and remediation.

Findings are documented, and a follow-up action plan established where corrective action requests are raised by Moorepay and remedial and preventive actions are provided by the supplier.

When necessary, an audit is undertaken to evaluate the effectiveness of the remedial actions proposed.

Managing changes to supplier services

A tiering system is used to ensure appropriate assessment of risk is undertaken. Where the provision of service by a supplier is changed, the suppliers associated tiering is reevaluated and the risk assessment aligned.

Information security incident management

Management of information security incidents and improvements

The following controls have been deployed to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Responsibilities and procedures

Moorepay has a formally documented Security Incident Management Standard Operating Procedure (SOP) which underpins the Security Incident Management policy.

The Security Incident Management SOP seeks to describe the Security Incident Management Process with a clarity to allow operational teams to establish and effectively operate the process and to implement the Security Incident Management policy.

A requirement of the Security Incident Management SOP is that a Security Incident Response Team (SIRT) should be formed from applicable areas of the business to ensure appropriate representation and executive sponsorship is provided to effectively respond to the incident.

The SIRT are responsible for the following activities throughout the life cycle of the security incident:

- the effective and timely response to the security incident
- attendance at SIRT meetings
- ensuring resource is available from the delegated business area as required
- ensuring the required priority and commitment is given to investigation and remediation activities
- ensuring communication to clients is managed effectively.
- escalating within the business when appropriate.

Reporting information security events

As part of the Analysis phase of the Security Incident Management SOP, a Security Incident Response Team (SIRT) is established to ensure effective management of the

incident and to ensure that applicable business owners and Senior Leadership are kept informed.

Communication to internal stakeholders is maintained throughout the process in the form of a regular security statement and provision of a detailed incident report as required.

In line with Article 33 of GDPR, "notification of a personal data breach to the supervisory authority" is the responsibility of the data controller and states that the controller's requirement is to notify the ICO within 72 hours, and that this time only begins once the controller has become aware of the breach. Similarly, notification (if required) to the affected data Subjects (where there is a high risk to the rights and freedoms of data subjects, is the responsibility of the data Controller (GDPR Article 34).

Article 33(2) applies to Moorepay (as the data processor) which states, “the processor shall notify the controller without undue delay after becoming aware of a personal data breach.”

As defined within the Security Incident Management process, and aligned to the GDPR, data breaches are reported to business owners and Senior Leadership, who ensure external communications to customers as soon as practically possible.

If known at the time, the following information will be supplied by Moorepay as part of the initial communication:

- description of the breach
- when and how Moorepay were informed of the breach
- the people that may have been affected by the breach
- summary of containment activities
- contact information for further information

A communication plan will then be agreed with the customer and implemented to ensure ongoing communication is upheld throughout the process.

Reporting information security weaknesses

There is a clearly defined process for reporting security events (including incidents and weaknesses), either directly to management or Security via the Service Desk.

Information on reporting security incidents and weaknesses is published on the corporate intranet, included in the annual e-learning compliance training and covered in local and central newsletters and awareness programs.

Assessment of and decision on information security events.

Upon notification of a potential security event, the event will be assessed by a Security team member during the Triage phase. If deemed appropriate based on initial.

Assessment of the facts, the event will be classified as a security incident and an appropriate incident response plan implemented.

Response to information security incidents

Moorepay has a formally documented Security Incident Management Standard Operating Procedure (SOP) which underpins the Security Incident Management policy.

For the purpose of the Security Incident Management SOP, an Information Security incident is defined as any irregular or adverse event that has resulted or may result in an unwanted impact on the security of information assets, business operations or information processed on behalf of clients. The term 'Incident' can apply to emergencies, legislative or contractual breaches, operational failures or abnormal situations or perceptions.

The Security Incident Management SOP is followed in all cases when a security incident is reported to the Security team, including in the events of a potential or realised cyber-attack or a data breach.

The Security Incident Management SOP end to end process incorporates the following process stages:

- analysis
- containment
- eradication
- recovery
- review
- reporting and communication

Learning from information security incidents

It is mandated in the Security Incident Management SOP that a detailed investigation is carried out with responsible colleagues and stakeholders. As part of the Eradication phase, Root Cause Analysis (RCA) is undertaken and observations and recommendations are submitted by the Security team to ensure that lessons are learned, and problems are addressed.

Collection of evidence

Moorepay's Forensic Investigation Management Standard establishes the security standard for Forensics management to maximise the ability to preserve and analyses data generated by an IT system that may be required for legal and regulatory purposes.

Evidence is collected and stored in a secure evidence repository.

When dealing with evidence, a Chain of Custody (CoC) is maintained throughout the entire lifecycle of the incident. Chain of Custody information is entered into the incident ticket notes each time evidence is handled, stored, gathered, or transferred. The following details are recorded as a minimum:

- what
- when
- where
- who
- how

Information security aspects of business continuity management

Information security continuity

The following controls have been deployed to ensure that information security continuity is embedded in Moorepay's business continuity management systems.

Planning information security continuity

Moorepay has a business resilience policy that describes the aims and objectives of the Business Continuity Management System (BCMS). These objectives support the Company business objectives in providing assurance that key products and services will be available when required by those parties authorised to have access.

The interested parties include customers, employees, legal authorities, partners and the Company owners.

The Business Continuity Management objectives are as follows:

- to assign appropriate roles and responsibilities for BC management, firstly to prepare for a major incident and then ensure that major incident response has the appropriate level of support from key business functions.
- to ensure that a comprehensive Business Impact Analysis (BIA) and risk assessment is completed for all critical activities, products and services.
- to ensure documented recovery plans are maintained and reviewed regularly for activities that deliver and support critical products and services.
- to conduct exercises and tests to an agreed schedule, ensuring that results are evaluated, and any shortcomings recorded with improvement actions documented and owners agreed.
- to ensure that all staff are given training appropriate to their role in the BCMS to ensure that they can fulfil their duties within the BCMS.
- to ensure that internal audits and management reviews are undertaken at agreed intervals to provide assurance that the BCMS is effective.

Moorepay has in place documented Data Centre Disaster Recovery (DR) plans. The objective of the DR plan is to ensure that Moorepay can restore all in-scope services, within their agreed recovery service levels, in response to a disruptive incident.

The plan provides application environment information, recovery requirements and tasks needed to fail-over to a secondary location. The plan incorporates the recovery plan for the hosted application environment.

The DR plan is designed to integrate with the Major Incident process, which must be followed when it has been determined that the DR plan needs to be initiated.

The DR Plan incorporates the following key information:

- service overview
- recovery actions
- recovery management team
- site details
- pre-emptive activities • recovery dependencies
- recovery procedures
- key contact

Recovery targets

The standard SLA allows 24 hours from a major outage to consider the invocation of DR. The Recovery Time Objective (RTO) is within 24 hours of a DR incident being invoked by Moorepay management. Maximum overall downtime is 48 hours.

The standard Recovery Point Objective (RPO) is guaranteed within 4 hours of a DR incident being invoked by Moorepay management.

Implementing information security continuity

Each Business Continuity and Disaster Recovery plan stipulates the requirement for information security controls to be applied to ensure the confidentiality, integrity and availability of information and systems is maintained during a disruptive incident.

Where applicable, specific instructions are included in recovery steps to ensure the continued implementation of security controls.

Emergency response teams are formed to coordinate Business Continuity and Disaster Recovery events, the teams include information security specialists to ensure that security is maintained throughout the recovery period.

Risk assessment is carried out and mitigating controls implemented where the effectiveness of security controls is reduced due to the disruptive incident.

Verify, review and evaluate information security continuity.

Application disaster recovery tests are performed at least annually or when significant changes occur within the hosting infrastructure to confirm recovery requirements can be met. Clients are invited to participate in recovery exercises. For additional information on DR testing please see MAP document 04 Business Continuity.

Redundancies

Availability of information processing facilities

Data centres are mirrored in a separate geographical location.

Infrastructure used to deliver the service has N+1 redundancy designed in at all levels to protect against component failure. The Data Centres are Tier 3 level, offering site wide resilience and suitable environmental controls to protect the availability of systems and data.

To provide a resilient connection between the customer site and Moorepay 's data centres; two IPSec VPN tunnels are created at installation time, one to the primary data centre and another to our secondary (DR) site.

Compliance

Compliance with legal and contractual requirements

The following controls have been deployed to ensure that legal, statutory, regulatory or contractual obligations related to information security are understood and upheld by stake holders.

Identification of applicable legislation and contractual requirements

Moorepay Compliance team monitors and tracks corporate legal and regulatory obligations including those requirements relevant to the ISMS.

Moorepay’s normal ISMS controls are designed to deliver customers standard contractual requirements. Where non-standard contractual requirements are identified, customer specific controls may be implemented within the individual customer delivery teams. Intellectual property rights.

Acceptable use of software is included in the Moorepay Acceptable Use policy.

Moorepay maintains a software asset register and has put in place a software auditing tool which are used to determine what software is installed and to ensure that Moorepay is adequately licensed for all software products and that employees have not installed unauthorised software.

Controls are deployed to ensure that users cannot install software without prior approval.

Moorepay only acquires software from known reputable sources to ensure that copyright is not violated.

Protection of records

Moorepay has a documented Information Classification and Ownership policy. The objective of the Policy is to identify and implement adequate and effective information handling and protection controls, appropriate to the sensitivity of the information being handled. The purpose being to ensure that the valuable business and personal information used within Moorepay and the information entrusted to the organisation by its customers is appropriately protected throughout its lifetime.

Privacy and protection of personally identifiable information

An essential activity within Moorepay is the processing of personal data of its client's employees, in order to operate effectively and provide its services. This is done in accordance with the applicable data protection and/or privacy laws of the countries in which it provides services.

The General Data Protection Regulation is used as the best practice standard in countries where there is no equivalent data protection and/or privacy law or regulation.

Local legislation may require a specific implementation of policies and practices to align with local legal requirement(s).

When acting as custodian of personal data, Moorepay ensures that the data is always handled properly and securely, irrespective of whether it is held in electronic or physical form, and covering the whole data lifecycle, including:

- the obtaining of personal data
- the storage and security of personal data
- the use of personal data

- the disposal/destruction of personal data

Moorepay and its group companies are registered with the Information Commissioners Office as follows:

- Zellis Holdings Ltd – registration number ZA331332
- Zellis UK Ltd – registration number Z6810325
- Moorepay Limited – registration number Z9176805
- Moorepay Compliance Limited – registration number ZA731897
- Benefex Ltd – registration number Z8773454
- Benefex Financial Solutions Limited – registration number Z3103927

Regulation of cryptographic controls

The Moorepay Information Handling standard mandates the requirements for the protection of information assets, system resources and information, in order to meet the legal and regulatory requirements of Moorepay, its clients and other stakeholders. The standard ensures that cryptographic controls are deployed where applicable.

The Moorepay Cryptography policy establishes the minimum security requirements for cryptography management.

Information security reviews

The following controls have been deployed to ensure that information security is implemented and operated in accordance with the Moorepay's policies and procedures.

Independent review of information security

Moorepay's approach to managing information security and its implementation, which include but it is not limited to, control objectives, controls, policies, standards and procedures, is reviewed independently at planned intervals, internally and externally by suitably qualified personnel.

Internal audits are performed by the Moorepay Security team and Compliance team independently.

Internal audits may be triggered by various events, including but not limited to the following:

- as part of the continuous audit program

- as part of root cause analysis and eradication and recovery activities of a security incident
- as part of risk assessment and remediation activities.
- as part of Change Management activities.

External audits are performed by independent third parties for the following,

ISO 27001:2013

Scope: Information Security Management System for the products and support activities to develop, support, handle, transfer, administer, store and process Payroll and Human Resource Information.

Cyber Essentials

Scope: Moorepay UK Limited Network Boundary and End Point Device's

Compliance with security policies and standards

Managers are required to participate in internal and external audit activities and are responsible for the creation and implementation of corrective actions to improve security control maturity.

Regular ISMS management review meetings are held, which include input from business leaders and a review of security risks. This process is checked and verified by BSI (British Standards Institute) for our certification to ISO 27001.

Technical compliance review

Security control assessments are defined and executed on a scheduled basis. Results of the assessments are reviewed by management and where applicable, audited annually by independent third-parties.

Document 3 - Data Protection Overview

Introduction

An essential activity within Moorepay is the processing of personal data of our client's employees, to operate effectively and provide our services. This is done in accordance with the applicable data protection and/or privacy laws of the countries in which we provide services.

The General Data Protection Regulation (GDPR) is used as the best practice standard in countries where there is no equivalent data protection and/or privacy law or regulation.

Local legislation may require a specific implementation of policies and practices to align with local legal requirement(s). For UK data subject, Moorepay aligns with the UK GDPR and the UK Data Protection Act 2018. For Irish data subjects (EU data subjects) the EU GDPR will apply.

When acting as custodian of personal data, Moorepay ensures that the data is always handled properly and securely, irrespective of whether it is held in electronic or physical form, and covering the whole data lifecycle, including:

- The obtaining of personal data
- The storage and security of personal data
- The use of personal data
- The disposal/destruction of personal data

This document seeks to consolidate relevant information on the implementation of practices and policies adopted by Moorepay to ensure the secure handling of data in line with applicable laws and regulations as outlined above.

Organisation

Moorepay General Counsel has overall responsibility for Legal and Compliance matters. The Legal team and Compliance & Auditing team report into the General Counsel.

The Head of Information & Cyber Security (HIS) is responsible and accountable for Information and Cyber Security within Moorepay, reporting directly to the Chief Information Security Officer (CISO).

An Information Security team and Technical Security team report in to the HIS.

Identification of applicable legislation

The Moorepay Legal and Compliance teams are responsible for tracking and monitoring the laws and regulations that impact the services that Moorepay delivers to its clients. They daily monitor in the areas of labour and employment, payroll, benefits, global mobility, recruiting, and data privacy and protection, among others, in all countries where clients have employee populations.

Information Commissioners Office (ICO) registration

Moorepay and its group companies are registered with the Information Commissioners Office as follows:

- Zellis Holdings Ltd – registration number ZA331332
- Zellis UK Ltd – registration number Z6810325
- Moorepay Limited – registration number Z9176805
- Moorepay Compliance Limited – registration number ZA731897
- Benefex Ltd – registration number Z8773454
- Benefex Financial Solutions Limited – registration number Z3103927

Data processing outside of the UK or the EU

Within its group of companies, Moorepay may transfer data across the globe to our various service delivery locations and offices. Depending on the type of data and the type of processing that is required or processed, this may include Moorepay suppliers and partners.

Moorepay rely on EU Model Clauses/Standard Contractual Clauses as the basis for its international data transfer agreements, both internally and externally.

Refer to the Customer Agreement for further details of processing locations and permissions.

Transparency (privacy information to customer data subjects)

Moorepay act as data Processor with respect to services delivered to its customers, and as such process Personal Data entirely under the instruction (general or specific) from the customer (who is the data Controller). It is therefore for the customer to conform with the transparency and notification requirements in the GDPR (GDPR Art 5(1a) and specifically the requirements for Privacy Notices in GDPR Art 12, Art 13 and Art 14 as applicable).

The customer should therefore provide suitable privacy information (e.g. Privacy Notices) to their employee/pensioners etc (i.e. the Data Subjects) which explains how their data is processed (including how the client uses the services of a third party data Processor if necessary (e.g. for SaaS or Managed Services).

Cyber insurance

Moorepay has Cyber Insurance cover which may cover certain losses in respect of cyber incidents.

Employee screening

Employee screening is mandatory before granting them any access to corporate assets. Background verification checks on all candidates for employment, contractors, and third party users are carried out in accordance with relevant local laws, regulations and to the business requirements. As part of the employment obligation, employees, contractors and third party users must agree and sign the terms and conditions of the employment contract, which state their and the organisation's responsibility for information security. Any failures will be dealt with by the Moorepay' disciplinary process.

Our standard vetting requirements are;

- Right to Work Check
- Proof of Residency Check
- Financial Probity Check
- 5 Years of Activity History
- Criminal Record Check

Dependent on the role of the employee, additional checks are carried out in line with our client's policies and requirements of specific clearance requirements.

Data protection requirements within employee contracts

Confidentiality clauses and requirement to comply with company policies are contained within standard contracts of employment and state the employee's requirement to maintain the confidentiality of the Company's sensitive technical and commercial information and information held in trust on behalf of a third parties.

Any failure to adhere to the terms and conditions of employment is dealt with by Moorepay' own disciplinary process appropriate for local legislation.

Awareness training

An Annual e-Learning security training framework is provided and is mandatory for all employees without exception and is also part of the employee induction process.

The objectives of the annual e-learning training framework include:

- Adhere to Moorepay security policies and standards.
- Understand key data privacy concepts important to the performance of your role.

All staff are tested on their knowledge of each subject and must attain an 80% pass mark to complete each module.

To supplement the annual training, the security team regularly deliver additional material focused on important aspect of security, providing further guidance on how to apply good practice and working in a more secure way.

Local divisions and departments are responsible for creating appropriate procedures and work instructions to ensure that processing and support activities are undertaken in a consistent manner and in line with applicable corporate policies and legal and regulatory requirements.

Technical and organisational measures

Moorepay has implemented appropriate and proportional technical and organisational measures to ensure the effective management of risks to information and information systems.

Security by design is incorporated into the design, development and acquisition of information systems.

Appropriate physical, logical and environmental controls are in place at Service centres and Data centres to prevent unauthorised access, damage and interference to information processing facilities, and Company and customer information.

Infrastructure used to deliver the service has N+1 redundancy designed in at all levels to protect against component failure.

Data encryption technologies are deployed where applicable.

Anti-malware technologies are deployed to all end point devices and servers.

Firewall and Intrusion Detection technologies are deployed throughout the hosting infrastructure and corporate network to protect against intrusion and denial of service attacks.

Penetration and vulnerability testing is conducted on systems and applications at defined intervals and systems are patched on a regular basis.

A Security Information and Event Management (SIEM) system is in operation, logging is enabled on systems, infrastructure and applications and events are monitored by the Security Operations Centre (SOC).

Control tests are conducted at defined intervals to ensure the effectiveness of security measures.

Moorepay has in place a formally documented Security Incident Management process and procedures which underpin the Security Incident Management policy.

The ability to maintain service delivery and restore systems during adverse situations is ensured by a Business Continuity Management programme. Business Continuity and Disaster Recovery plans are maintained and tested at regular intervals.

Moorepay has an Information Security Management System (ISMS) which is aligned with the international standards and code of practice ISO 27002. Moorepay security controls are based on industry best practice and aligned with ISO 27001. Moorepay is certified to ISO 27001:2013 standard, the overall requirement of which are:

Risk Management

- Legal and Regulatory Compliance

Business Continuity

- Security Awareness
- Security Incident and Weakness Management
- Supplier Management

Access to systems is governed by Logical Access Management and Physical Access Management Policies.

Regular prescribed checks are performed on user profiles quarterly, to ensures that staff have been assigned right level of privileges as per their job role and responsibilities.

Segregation of duties is implemented to reduce the reliance on key individuals and to prevent errors, and fraud.

Information security management policy

The Moorepay Information Security Management Policy sets out the organisation's approach to managing its information security objectives.

The Policy sets out Moorepay' strategic commitment to information security management that:

- Ensures the continued quality of service

- Meets the organisation's contractual, legal and regulatory obligations
- Meets the needs and expectations of clients and other interested parties The primary objectives of this Policy are to:
- Protect Moorepay and its customers' information assets from all threats, whether internal or external, deliberate or accidental
- Minimise the risk of damage by seeking to prevent the occurrence of security incidents and reducing their potential impact

The Information Security Management policy is supported by a set of topic specific policies, standards, guides, processes and other documentation. A summary of this policy set is available upon request.

Data protection policy

Moorepay has a documented Data Protection policy that applies to all personal data that is processed by the company, including personal data of its client's employees.

The purpose of the policy is to ensure that Moorepay:

- Comply with applicable data protection and privacy law and follow good practice
- Protect the rights of our employees, clients and their employees and its partners
- Is open about how it stores and processes data; and
- Protects itself from the risks of a data breach

The policy stipulates that as a minimum, Moorepay must ensure that:

- Only individuals who are authorised to use information can access it;
- Information is accurate and suitable for the purpose for which it is being processed
- Authorised persons can access information if they need it for authorised purposes; and
- Personal data is never stored or transported on a laptop, mobile phone or removable storage device, nor sent unencrypted through any channel (unless a recorded exception applies)

The policy covers the following topics:

- Responsibilities
- Data retention
- Data privacy principles and rights
- Cookies and third party data
- International data transfer

Privacy by design

Privacy by Design holds that organisations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

Moorepay promote a Privacy by design approach through:

- Training and awareness: by ensuring that all relevant staff are aware of the obligations and risks to privacy so that this knowledge permeates the development process;
- Our technical and organisational measures as detailed elsewhere in this document;
- Adopting a privacy first approach;
- Tools such as Data Protection Impact Assessments (DPIA) or other risk assessment tools as necessary or useful.

The Moorepay Secure Application Development Policy applies to the acquisition, development and maintenance of all software, systems, equipment and services which support Moorepay information assets. All of Moorepay IT system development activities and suppliers providing information systems and services to Moorepay are required to comply with this Policy.

The objectives of secure application development are:

- To build information security into the entire lifecycle of application acquisition, development and maintenance.
- To make sure that when information systems are designed and implemented, information security is an integral part of the lifecycle.
- To build appropriate levels of protection of data used for testing information systems.

The Moorepay Technical Advisory Board (TAB) validates proposals for new technology. As part of the review process, Security and Compliance subject experts provide input to ensure that:

- Legal and Regulatory requirements are understood by stake holders.
- Sufficient Security and Privacy controls are incorporated into the proposed solution.
- Any projects that involve handling Personal Data may be subject to a Data Privacy Impact Assessment (DPIA).

As part of the Software Development Lifecycle (SDLC), quality assurance and regular code review ensures that any potential security vulnerabilities are identified and addressed prior to the application being released into the production environment.

Code reviews incorporate static code analysis checks for OWASP Top 10 vulnerabilities as well coding standards adherence.

The SDLC process ensures that each software enhancement is subjected to a series of control point checks and approvals before release into Production. A DPIA may be a mandated requirement within this process.

Developers work closely with third-party security experts who advise of best practice guidance on safe coding techniques, as part of the SDLC, and is done within scope of the vulnerability management programme.

Data classification

Moorepay has a documented Information Classification and Ownership policy. The objective of the Policy is to identify and implement adequate and effective information handling and protection controls, appropriate to the sensitivity of the information being handled. The purpose being to ensure that the valuable business and personal

information used within Moorepay and the information entrusted to the organisation by its customers is appropriately protected throughout its lifetime.

This Policy is supported by the Information Handling Standard which outlines the rules for handling information throughout each stage of its lifecycle.

Information must be classified as one of the following four categories:

- Public

Information that is freely available. This is identified where no document label is present or by any document label that has none of following classifications.

- Company restricted for internal use only

Information classified as Company Restricted for internal can be released to any company employee or authorised and approved contractor.

- Company or client confidential

All personally identifiable information handled, processed or stored by the Company or on behalf of the Company.

- Company secret

Information which if released would have a significant impact on the Company's reputation and commercial success.

Access to customer data

Moorepay service operations employees, and approved partners that have been assigned to deliver the service will have access to the customer Information. For a SaaS implementation the majority of access to data will be by the customers personnel only; however, Moorepay system administrators and support staff may also have indirect

access to data. Controls are in place to manage this type of privileged user access.

Data Privacy requirements within supplier contracts

Security requirements are addressed via Contracts, Statement of work and Strategic partnership agreement.

Standard contracts stipulate that suppliers must comply with laws and regulations regarding data privacy and data protection, including but not limited to the GDPR / Data protection Act 2018.

It is mandated that suppliers must comply with Moorepay's Abridged Data Privacy Policy and Security and Compliance Standard for Outsourced Third Party Service.

Providers and must implement and maintain appropriate technical and organisational measures and other protections for Personal Data, in areas including but not limited to the following:

Risk Management

- User Awareness
- Incident and Change Management
- User Access
- Data Protection
- Physical Security

Business Continuity and Disaster Recovery

- Cryptography
- Vulnerability Management

Third parties risk assessment

Risk assessment is completed prior to the granting of access rights to third parties. The risk assessment must include a Privacy Impact Assessment in cases where Personal Information is to be stored, processed or transmitted.

Ongoing assessments of critical suppliers is undertaken to ensure the continued alignment of controls within supplier contracts. The right to audit is written into standard supplier contracts.

Third party sub-processors

Details of sub-processors which may be used by Moorepay are maintained and either detailed in the specific service contract and/or as detailed at the following online document:

Further information may be supplied by the relevant account management representative.

Data storage

Generally, all customer data is stored on encrypted storage within the secure data centre environment. It is possible that Payroll and/or HR functions (where an outsourced service is provided) may retain data locally for specific processing reasons.

Controls are in place to protect the data in these circumstances.

Desktop computers used in the delivery of the service have standard builds deployed that incorporate restricting access to USB drives, CD/DVD drives and local hard drives, preventing data being stored locally.

All laptops and mobile devices have whole disk encryption enforced. All removable media is encrypted to standards mandated in the Moorepay Cryptography Policy.

Removable media is secured adequately when not in use, in line with the controls stipulated for the classification of data contained on the media.

Data retention

When processing client's employee data, Moorepay are acting as the data Processor, and as such it is for the data Controller (the client) to ultimately determine the data retention and destruction of their data.

Data is kept only for as long as is necessary to provide the stated services and fulfil legal, regulatory, and contractual obligations; otherwise the data is returned or destroyed.

Refer to the Customer Agreement for further details of data retention.

Data destruction

The SaaS server environments utilise shared file systems, therefore at the end of service the customer data is removed, and the storage is returned to shared SaaS environment.

A manual process is followed to remove customer data, whereby the application and database instances are removed. and any dedicated file systems the customer may have are deleted. Customer backup data is deleted as part of this termination process.

Where customers have dedicated virtual disk volumes on the SAN, the volumes can be deleted at the end of the service. The physical disks are then made available to other virtual volumes.

To remove Information and software from equipment before destruction, a sanitation program is used.

Confidential information on hard copy marked for destruction is stored in secure bins prior to destruction. The hard copies are destroyed by secure shredding methods by approved third parties. A certificate of disposal is issued by the third party and maintained by Moorepay for inspection and audit.

Data collection

If data is collected directly from the Data Subject through the service, then the client must ensure that there is a valid legal basis for collecting that data.

Data transfer

Data transfer between the data centres and client PC's are secured using HTTPS and Digital Certificates.

Interface file transfer is provisioned via an SFTP Portal that uses unique credentials per customer.

Risk management

To ensure that the valuable business information and information processing assets used within Moorepay and the information entrusted to the organisation by its clients

and business partners is appropriately protected throughout its lifetime, the Company operates a formal information security risk governance structure and risk management model to ensure that:

- The Company is able to make informed decisions on the treatment of information security risk
- Acceptance and management of identified information security risk is undertaken by those authorised to do so
- A consistent and repeatable methodology for the assessment of information security risk is adopted
- Ownership of risk and risk treatment actions is formally assigned

The implementation of the Company's information security risk strategy is based on formal and repeatable methods for risk assessment, risk management and risk acceptance.

Projects that aim to handle Personal Data may be subject to a Data Protection Impact Assessment (DPIA).

Critical assets are categorised for Risk Assessment e.g. Vendors, IT Infrastructure, Data Centres, and the associated threats, vulnerabilities and impacts considered. This is a broad assessment for each category of critical asset. If there is a need to take a more specific review of a single critical asset, then a review will be undertaken, and the output added to the risk register for ongoing management.

Identified security risks are reviewed as part of a regular ISMS management review and where appropriate a formal risk assessment undertaken. The risk assessment will be documented and submitted to the Head of Security (HoS) and Information Security Manager who will review the assessment. If approved, the HoS will inform the Risk Owner (usually an Extended Leadership Team member) and recommend a Risk Treatment option.

Data breach response

In the event of a suspected or realised data breach, Moorepay will follow its established Security Incident Management process.

The process seeks to describe the Security Incident Management Process with a clarity to allow operational teams to establish and effectively operate the process and implement the Security Incident Management policy. The process incorporates the

following process stages:

- Analysis
- Containment
- Eradication
- Recovery
- Review
- Reporting & Communication

In line with Article 33 of GDPR, "Notification of a personal data breach to the supervisory authority" is the responsibility of the data controller and states that the controller's requirement is to notify the ICO within 72 hours, and that this time only begins once the controller has become aware of the breach. Similarly, notification (if required) to the affected data Subjects (where there is a high risk to the rights and freedoms of data subjects), is the responsibility of the data Controller (GDPR Art 34).

Art 33(2) applies to Moorepay which states, "The processor shall notify the controller without undue delay after becoming aware of a personal data breach."

As defined within the Security Incident Management process, and aligned to the GDPR, data breaches are reported to business owners and Senior Leadership, who ensure external communications to customers as soon as practically possible.

If known at the time, the following information will be supplied by Moorepay as part of the initial communication:

- Description of the breach
- When and how Moorepay were informed of the breach
- The people that may have been affected by the breach
- Summary of containment activities
- Contact information for further information

A communication plan will then be agreed with the customer and implemented to ensure ongoing communication is upheld throughout the process.

Regulatory alignment Context

As defined by the GDPR and DPA 2018, Moorepay is the Data Processor when handling customer data in the delivery of services to its clients (who are the data Controllers).

Legal basis

As a data Processor, it is not for Moorepay to determine the legal basis for processing client personal data. The client's data subjects are likely to be employees and as such they may well be processing the personal data as part of the employment contract; in order to comply with legislation or legitimate interest/public task (or such other legal basis detailed in Art 6 GDPR).

Where sensitive personal data (special category) is processed then additional legal basis(es) may be required as detailed in Art 9 GDPR and in Sections 10 & 11 of the Data Protection Act 2018 (UK).

For all cases it will be for the Controller (the customer) to determine (and notify to the Data Subjects through the Controllers Privacy Notices) the applicable legal basis for processing.

Processing purpose

Our clients (as the data Controller) will need to determine (and communicate to their Data Subjects through Privacy Notices) the purpose for which they are processing the data (even though they are using a third party for HR and payroll processing)

Data consolidation

Data from multiple sources may be interlinked and cross referenced within the various components of the product offering.

Details of the specific service design will be included in service contracts. Further information may be supplied by the relevant account management representative.

Data subject categories

Moorepay processes information for its customers typically for the following data subject categories.

- Applicants to the customer
- Employees of the customer
- Ex-employees of the customer
- Next of kin of the above

Data types

Personal data that Moorepay process may include the following:

- Name

- Home contact information (address and telephone number)
- Date and place of birth
- Gender
- Entitlement to residency
- Citizenship
- Passport number
- Emails and/or other documents and data in electronic form
- Bank account details and other financial information
- Family status
- Details of dependents
- Emergency contact name and address and telephone number
- Location
- Band/seniority, Work Level
- Salary plan information
- Associate ID number
- Department
- Line and sub-line of business
- Local Bank entity name
- Work contact information (telephone number, address, fax number and email address)
- Other address information, where appropriate such as temporary residence
- Cost centre information
- Start date and end date (if applicable) of employment
- Career relevant dates, such as promotion and rehiring events
- Reporting structure
- Benefits records and related information
- Time and Attendance information, including overtime, shift premiums, substitutions
- Working patterns and contracted working hours, including full time/part time indicators
- Information related to redundancy
- Employment history
- Language(s) spoken
- Garnishment information and recipients of garnishments
- Pension information, including pension plan and contribution
- Performance related information (current and historic including bonus rewards and individual objectives)

- Personal development plan information (including personal strength and weaknesses/development areas and assessment of potential)
- Information regarding entitlement to work including visas
- Tax and national insurance/social security details
- Information related to termination of employment

Moorepay may also process the following special categories of information:

- Personal data revealing racial or ethnical origin;
- Personal data revealing political opinions;
- Personal data revealing religious or philosophical beliefs (including any processing operations necessary to conduct tax filings);
- Personal data revealing trade union memberships (including payments, position and bank information);
- Personal data of genetic or biometric nature;
- Personal data concerning health information;
- Personal data revealing a natural person's sex life or sexual orientation; or
- Personal data revealing details regarding the (alleged) criminal commission or any offence including details of any proceedings of the sentence of a court

Data of children

It is not envisaged that data Controllers will use Moorepay services to process children's data. However, where that does happen it is for the data Controller to ensure that suitable transparency and legal basis determination is complied with.

Data subject rights (including subject access rights)

The data Controller is responsible for complying with any data subject right (e.g. SAR, Rectification, Erasure, Restriction, Portability, Object).

Where required, Moorepay as the data Processor will execute instructions from the data Controller to meet the GDPR requirements with respect to any rights request. Any requests from Data Subjects (i.e. employees of our clients) should be sent to the data Controller.

Inbuilt system functionality and robust operational procedures ensure that Moorepay can execute instructions from the data Controller in regard to data subject rights.

Rights in relation to automated decision making and profiling.

Automated decision making is only used where necessary to provide the contracted service. Customer data is not used for profiling.

Records of processing activities (RoPA)

Article 30 of the GDPR requires Moorepay as a Processor to maintain records of:

- Our name and contact details.
- The name and contact details of each controller on whose behalf we are acting (the Controller is our customer and is the organisation that decides why and how the personal data is processed).
- If applicable, the name and contact details of each Controller's representative (another organisation that represents the Controller if they are based outside the EU but monitor or offer services to people in the EU).
- The categories of processing we carry out on behalf of each Controller – the types of things we do with the personal data, e.g. payroll processing, HR admin services.
- If applicable, the name of any third countries or international organisations that we transfer personal data to (any country or organisation outside the EU).
- If applicable, the safeguards in place for exceptional transfers of personal data to third countries or international organisations. An exceptional transfer is a non-repetitive transfer of a small number of people's personal data, which is based on a compelling business need, as referred to in the second paragraph of Article 49(1) of the GDPR. (Note: It is unlikely we would ever need to execute an exceptional transfer).
- If possible, a general description of the technical and organisational security measures (our safeguards for protecting personal data, e.g. encryption, access controls, training etc).

Much of this information is also contained within the customer contractual documentation (including the MAP).

Note: Our customers (the data Controllers) are also required to maintain a RoPA for the Personal Data we are processing. The Controller's RoPA will contain more detail about the legal basis for processing etc.

Data extract / return

Where customer data is returned, the standard process is to extract the data and provide in Oracle Extract format. Alternative formats can be provided upon agreement.

Pseudonymisation and anonymisation

Where appropriate pseudonymisation or anonymisation techniques will be applied to Personal Data to minimise identification risk.

Accuracy of data

For SaaS services, the customer is responsible for accuracy of data.

HR and Payroll systems used in the delivery of the service have validation checks inbuilt to assist in ensuring accuracy of data.

Operational procedures have validation steps incorporated to ensure accuracy when processing customer data.

Privacy Notices

Details of how Moorepay use customer data (e.g. customer contacts etc) as a data Controller can be found in our Privacy Notices accessed from our websites at:

Document 4 - Moorepay Business Continuity

Introduction

This document forms part of Moorepay Assurance Pack (MAP) and should be viewed along with all other documents and artefacts included in the MAP to gain an overall understanding of the Moorepay security program.

The document is intended to provide an insight into Zellis business continuity planning and provide a high level illustration of:

- leadership commitment
- the approach to business continuity planning and assessment • the associated collateral
- impact assessments
- testing overview

Leadership statement

Moorepay are firmly committed to delivering our services and solutions to the highest possible standard, without putting the health and wellbeing of our colleagues or our customers at risk.

Where a pandemic event is declared there are a number of key considerations to take and a range of scenarios which could materialise.

Our response and contingency plans are continually reviewed and adjusted to align with guidelines published by WHO and by government.

Our key third party suppliers in our supply chain are fully engaged with Moorepay to ensure they have appropriate business continuity plans in place.

Approach

The Business Continuity Management (BCM) objectives are as follows:

- To assign appropriate roles and responsibilities for business continuity management, to prepare for a major incident and to ensure that major incident response has the appropriate level of support from key business functions.
- To ensure that a comprehensive Business Impact Analysis (BIA) and risk assessment is completed for all critical activities, products and services.
- To ensure documented recovery plans are maintained and reviewed regularly for activities that deliver and support critical products and services.
- To conduct exercises and tests to an agreed schedule, ensuring that results are evaluated, and any shortcomings recorded with improvement actions documented and owners agreed.
- To ensure that all staff are given appropriate training to fulfil their duties within BCM preparation and response activities.
- To ensure that internal audits and management reviews are undertaken at agreed intervals to provide assurance that the BCM System is effective.

BCM collateral

The following documentation types are incorporated into Business Continuity planning:

Policy

The Moorepay Business Continuity policy describes the aims and objectives of the Moorepay Business Continuity Management System (BCMS), and mandates the policy requirements in terms of the following:

- Responsibilities

Information security considerations

- Business impact analysis and risk assessment
- Contingency planning and response
- Testing

Business continuity assessment and planning

The Assessment and Planning document contains the results of threat assessments and business impact analysis as described in the Impact Assessment section of this document.

Moorepay uses a PESTEL approach to business impact analysis, whereby threat factors within the following areas are considered - Political, Economic, Social, Technological, Environmental and Legal.

Risk calculations follow the standard Moorepay risk management methodology to ensure consistency and repeatability.

Playbook

A fact based planning document providing an inventory of resources, capacity, supplies and service dependencies to be used with the Runbook.

Runbook

The runbook is a practical process based instruction guide to managing incidents pre-invocation and post invocation, and includes the following information:

- Process flowcharts which follow a risk based approach
- The step by step sequence of activities to be undertaken if a business continuity event is declared
- Clearly defined roles and responsibilities for each process step
- Detailed instructions for each process step The runbooks are practical and user friendly.

Impact assessment

Impact assessment is undertaken as part of Business Continuity planning. Threat sources, threat factors and vulnerability factors are defined for each BC scenario, and may include but are not limited to the following areas:

- Risk of damage or denial of access to sites
- Unavailability of Key Staff
- Unavailability of critical IT infrastructure and technology
- Unavailability of critical supplier services

Risks are identified and mitigation steps defined and incorporated into the Business Continuity planning.

Where required, Data Privacy Impact Assessments (DPIA's) are undertaken to define the relevant data flows and processing activities.

Business Impact Analysis is conducted against each service delivered from the site and takes into consideration the following:

- Maximum Time Without Service (MTWS) – the maximum time that the Business could continue without this activity being done.
- Recovery Time Objective (RTO) - the planned time that the service will be available after disruption.

Business Impacts Analysis and associated recovery planning ensures that there is sufficient contingency between the RTO and MTWS for the RTO to be achievable.

Exercises are conducted to ensure that the RTO remains achievable and that continual improvement activities widen the gap between RTO and MTWS to give sufficient contingency.

Business continuity testing

Business Continuity tests are designed to;

- Probe and evaluate the robustness of our plans
- Raise awareness and educate employees on how to react during business continuity
- Test abilities to bring the situation back under control as quickly as possible
- Identify new threats and assess them using our risk-based methodology
- Seize opportunities for improvement to enhance our business continuity planning and disaster recovery plans

Disaster recovery plan testing Private cloud

Application disaster recovery tests are performed at least annually or when significant changes occur within the hosting infrastructure to confirm recovery requirements can be met. Clients are invited to participate in recovery exercises.

Disaster recovery testing is conducted at the secondary data centre.

Data is replicated at the SAN layer from the primary to the secondary data centre on a 24/7 basis, this data is used in the recovery tests.

A point in time copy is taken of the data and mapped to the host profiles of the servers to be recovered.

The servers are brought online, a set of pre-defined tests are then run against the systems and a like for like comparison taken against the applicable servers at the primary data centre.

Test restores of data from the backup system are undertaken and tested to confirm the integrity of the data and effectiveness of the backup solution.

Upon completion of the infrastructure recovery testing, the Application and DB teams conduct the required restores and present the recovered applications to the customers and internal teams for individual application testing.

The overall end to end restore time is taken and measured against the published RTO of 24 hours.

RTO is calculated based upon a complete return to service of all platforms and does not consider individual systems.

Participating customers are provided with a summary report at the end of testing.

Document 5 - Moorepay Application Security Overview

Introduction

This document forms part of Moorepay Assurance Pack (MAP) and should be viewed along with all other documents and artefacts included in the MAP to gain an overall understanding of the Moorepay security program.

The security of Moorepay and HRWize's applications is a matter of the highest priority due to the sensitive nature of the data presented to users. This document seeks to provide an overview of the security features available within both applications and system design.

Moorepay Identity & access management Secure log-in functionality

Authorisation is always performed within Moorepay, there is a single stage where a user must provide a username, password. The user's security profile is referenced to determine a user's access rights. Authentication is provided from within Moorepay's Identity Service which can link externally or within the application.

Invalid login messages do not identify whether it is the username or password which is incorrect.

IP whitelisting is available and can be applied to users, this can be any public IP address or CIDR range.

Multi-factor authentication (MFA) is available as an option (subject to service offering) which adds an extra layer of protection on top of your username and password.

Single sign-on

Moorepay supports single sign on using OpenID Connect through the Moorepay identity Service.

OpenID Connect is an authentication layer built on top of the Oauth2.0 framework using a JSON (JavaScript Object Notation) web token to validates a user's authenticity, this allows the user to access websites and apps without having to login or share their sign in information again.

Moorepay also supports USB token based single sign on using Moorepay Identity Services.

Multi factor authentication (MFA)

The login process with username and password authenticates the user with "What they know". MFA introduces an extra level of authentication with "What they have".

Our solution incorporates industry standard security mechanisms, you can switch MFA on Moorepay and select one or both of two methods of secondary authentication. Both receive One Time Passcodes for the user to enter on login.

When authenticating against a corporate domain such as Azure Active Directory (AAD) any MFA in place such as Microsoft Authenticator will be inherited and be prompted when the user logs in to the domain.

Moorepay password policy

Within Moorepay the password functionality cannot be reset as it is a global setting with the application, the password policy consists of:

- Minimum Length 9
- Maximum length 128
- Maximum login on attempts of 5, with timed lockout.

- Minimum number of upper-case alphabetic characters of 1
- Minimum Numeric and symbol characters 1 of each
- A password mask.

Moorepay customers can define their own password policy by using Single Sign On to their corporate domain.

Security question

Moorepay requires the user to answer secret questions for password resets when not using Single Sign On. The password reset will send a timed Token to the user in order to

be able to reset their password after correctly answering their secret security questions which are set at first login.

Administrator Role

There is a separate administration module within Moorepay that handles users and security. Users with profiles including the administration module can perform the following administrative tasks:

Moorepay

- Access to security profiles
- Limit operator access to employees' records via security profiles
- Set up new operators and assign security profile
- Change the security profile attached to an operator
- Change a password for an Moorepay operator
- Run query tool reports

Moorepay Me

- Allocate, change or suspend a password for an employee

Moorepay access to data

Moorepay service operations employees, and approved partners that have been assigned to deliver the service may have access to the customer Information for the purpose of fulfilling their roles within the agreed context of the service.

For a Moorepay software implementation majority of access to data will be by the customers personnel only; however, Moorepay system administrators and support staff may also have indirect access to data.

Robust access controls are in place to manage Moorepay access to customer data, ensuring that:

- Access is approved before being allocated
- Access is allocated on a “need to use” basis
- Access is time based and allocation is reviewed regularly
- Activity is monitored

Moorepay Application Auditing

Auditing within Moorepay is partly configurable and under the control of the Moorepay team.

Moorepay uses tasks and database tables to enter and store data.

- a task is a set of screens that you can set up to enable you to ensure the correct screens are available for the task you are looking to perform
- a table or file is at database level, and is used to store specific data associated with a record within the system

Within tasks there will be different tables for each set of data. i.e. there will be a table to hold tax information and different table(s) for personal information.

Audit records include old and new value, date and time of the change, and the operator making the change.

Extractor can be used to interrogate audit data.

Moorepay Me changes can also be audited via the same mechanism.

Moorepay Encryption

Data storage encryption (at rest)

Moorepay databases reside on SAN storage that is encrypted using whole disc

encryption. At the time of writing the encryption cyphers deployed are to AES-256 standard.

Password protection

Passwords are stored in the Moorepay Identity Service Database.

Moorepay Identity Server uses a one-way hash with PBKDF2 with HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations.

HTTPS and SSL

Moorepay is configured by default to only allow access via HTTPS.

HTTPS encrypts and decrypts the page requests and page information between the

client's browser and the web server using a Secure Socket Layer (SSL). HTTPS by default uses port 443 as opposed to the standard HTTP port of 80. URLs beginning with HTTPS

indicate that the connection between client and browser is encrypted using SSL. Implementing SSL and using HTPPS provides a much greater level of security than submitting requests via HTTP alone.

Internet file transfer

Internet file transfer is provisioned via an SFTP Portal for customers that do not use the Moorepay Payroll application, the SFTP Portal uses unique credentials per customer. SFTP and FTPS protocols use SSL/TLS/SSH encryption algorithms with a 256 key length where the target systems allow.

Moorepay Session cookies

Moorepay is configured by default to use session cookies to maintain session affinity.

Once logged in, each application will establish a simple session cookie so that the user's details are "remembered" between page requests.

The default session expiry is set at thirty minutes of inactivity for Moorepay. This is generally agreed to be the optimum time for this type of application so that standard employee and manager HR tasks are not impacted.

Data retention

By default, data will be retained for the time a customer is under contract, data can be deleted in line with HMRC guidelines and leavers can be deleted after 4 years as per employer data retention periods.

Data deletion

The GDPR module provided as part of Moorepay provides the following data deletion functionality:

- Bulk Deletion Leavers, applicants and External Personnel
- Individual Deletion

Data Subject Requests

Specific tasks are available within the GDPR module of Moorepay which allow authorised users to run reports on all data associated with a specific user.

Moorepay Architecture Data segmentation

A dedicated Moorepay applications environment is shared between customers within our Azure Tenant. Dedicated data schema and file systems are provided per customer within our virtualised infrastructure. This provides substantial safeguards for data privacy and security and means that data is not co-mingled with other customers. Significant safeguards for data privacy and security are deployed within the hosted environment; for example, each service is allocated its own subnet address range, its own ruleset on our edge firewalls.

Network segregation

Moorepay is made up of the following service delivery tiers:

- Presentation (MVC)
- API
- Micro Services
- Business logic/batch processing services
- Database

Logical segregation is implemented to separate each delivery tier.

Application Architecture

HRWize Identity & access management Secure log-in functionality

Authorisation is always performed within HRWize, there is a single stage where a user must provide a username and password or username, password and PIN.

- This is a 6-digit PIN number and the user is asked to enter 3 random digits from that PIN number.
- PIN login is turned on globally and you have two options – all users OR only HR and admin level users

The user's security profile is referenced to determine a user's access rights. Authentication is provided from within the application.

Invalid login messages do not identify whether it is the username or password which is incorrect.

The login pages are protected using Google reCaptcha v3 – this is a transparent process (as opposed to the older versions which ask you to enter letters or click on fire hydrants etc).

IP whitelisting is available and can be applied to users, this can be any public IP address or CIDR range.

Multi-factor authentication (MFA) is available as an option (subject to service offering) which adds an extra layer of protection on top of your username and password.

Single sign-on

HRWize supports single sign on to various different Identity providers, listed below;

- Azure Active Directory
- Okta
- OnleLogin
- Google oAuth
- Google SAML

Multi factor authentication (MFA)

The login process with username and password authenticates the user with "What they know". MFA introduces an extra level of authentication with "What they have".

Our solution incorporates industry standard security mechanisms, you can switch MFA on HRWize and authentication is based on QR Codes using various authenticator apps such as Microsoft Authenticator, Google Authenticator or Authy.

MFA login can be turned on globally for all users or specifically for HR and Administrator users only.

When authenticating against a corporate domain such as Azure Active Directory (AAD) any MFA in place such as Microsoft Authenticator will be inherited and be prompted when the user logs in to the domain.

HRWize password policy

- Within HRWize the password Customers can configure certain elements of their password policy.
- Minimum Length – Customer Configurable - minimum 8
- No maximum length
- Maximum login on attempts of 5, with timed lockout. 15 attempts blocks IP.
- Forced Password Change – Customer Configurable

HRWize customers can fully define their own password policy by using Single Sign On to their corporate domain.

Moorepay/HRWize access to data

For a HRWize implementation majority of access to data will be by the customers personnel only; however, HRWize system administrators, implementation and support staff may also have indirect access to customer data.

Robust access controls are in place to manage Moorepay/HRWize access to customer data, ensuring that:

- Access is approved before being allocated
- Access is allocated on a “need to use” basis
- Access is time based and allocation is reviewed regularly
- Activity is monitored

HRWize Application Auditing

Within HRWize, there is an auditing function which audits all actions which result in a change to the database – that is to say all write, update and delete actions. Other significant actions such as logins, running a report, downloading form data and viewing documents are also audited.

The audit log is only visible to Administrator level users. The information can be accessed via the audit module as well as via reporting.

The format of an audit record is:

Datetime – this is always recorded in UTC Username

IP address

Action – the exact format will vary according to the use case but generally this will follow the format of “Bank details updated: Phoebe Parker (47)” or “Added time off: Sickness (2023-07-20 – 2023-07-21) Aimee Hancock (G7LQE7) (390)”

HRWize Encryption

Data storage encryption (at rest)

HRWize databases are encrypted at rest - at the time of writing the encryption cyphers deployed are to AES-256 standard.

Additionally, specific fields in the database are encrypted at a field level – these are:

- National insurance number
- Date of birth
- Bank account sort code
- Bank account number
- Bank IBAN
- Bank Swift code
- Driving license number
- Passport number

Password protection

Passwords are stored in the HRWize Application Database. Passwords are salted and hashed using BCrypt with a cost of 10. HTTPS and SSL.

HRWize is configured by default to only allow access via HTTPS.

HTTPS encrypts and decrypts the page requests and page information between the client’s browser and the web server using a Transport Layer Security (TLS 1.2), formerly Secure Socket Layer (SSL). HTTPS by default uses port 443 as opposed to the standard HTTP port of 80. URLs beginning with HTTPS indicate that the connection between client and browser is encrypted using TLS 1.2. Implementing TLS 1.2 and using HTPPS provides a much greater level of security than submitting requests via HTTP alone.

HRWize Session cookies

HRWize uses session cookies to maintain session affinity. Once logged in, each application will establish a simple session cookie so that the user's details are "remembered" between page requests.

The cookie in use is an HTTP cookie and we use a Secure cookie.

The default session expiry is set at thirty minutes of inactivity but this can be changed by the company to a maximum of 240 minutes (4 hours).

HRWize Data Management Data retention and deletion

HRWize does not delete any client data and, therefore, the retention of data is infinite should the client so choose – as data processor, we will only ever act in accordance with the instructions of the data controller.

Should you opt to delete data, you can remove individual records via the relevant modules in HRWize – additionally, many of these modules have the ability to bulk select and delete records to make this process quicker.

When deleting data this will, in the main, only delete that record – for example a training request. However, should you delete an employee this will remove the employee and ALL associated records including documents.

Data Subject Access Requests

Should a subject make a subject access request, HRWize allows the data controller to perform a system wide search based on the employee entity – note this will not find instances of the employee being referenced in another record (i.e., if their name is mentioned in someone else's performance appraisal then this will not be included).

Once the search is completed, you can then download all of the data contained in the system to HTML, PDF or XML allowing you to then share with the subject once you have confirmed the contents in accordance with your policies.

HRWize Architecture

Customer Data segmentation

HRWize's Database is multi tenanted with data segregation using unique identifiers per customer and application security.

Network segregation

HRWize is made up of the following service delivery tiers:

- Application
- API
- Database

Application Architecture

Data Centres

All data centres used to provide HRWize services are located in the UK.

Services are provisioned in a combination of Azure data centres, utilising public cloud offerings, and separate third-party data centres housing hardware and software assets that are leased, owned, managed and maintained by Moorepay/HRWize.