Information Management Policy

Ver 1.0

Date 17th May 2023

Spinwell's Information Management System has been created using the ISO 27001:2013 methodology and as such, Spinwell are accredited to ISO 27001:2013. Due to our requirement for advanced data security we also hold Cyber Essential Plus and our systems have been vetted and deemed to meet Government Security standards. As such our ISMS Aspects Directives acts as our Information Management Policy and where necessary we have strengthened some of the Directives in order to meet our security obligations. Some subject areas of this policy may also have their own policy documents as required.

ISO 27001:2013

ISMS Aspects Directives for Spinwell Global Limited

This document should be read in conjunction with the ISMS Aspects Policies.

Last Modified:	08/11/2022
Modifier:	
Version:	1.3
Document URL:	ISO 27001:2013 - 2021 ISMS Aspects Directives

Index of Contents

ISMS Aspects Directives

Purpose

This document defines our high-level Information Security Directives aligned to the International Standard for Information Security using ISO 27001:2013, ISO 27002:2013 and other relevant Standards. This document should be read in conjunction with the ISMS Aspects Policies which establish the policy position for the different aspects for the Company.

These Information Security Directives have been benchmarked against the Standard as well as industry best practice to ensure that they are comprehensive and appropriate.

Risk-based approach

These Directives take a risk-based approach. The principles behind this approach are:

- A baseline set of controls is defined which are applied to all Information Assets
- More sensitive assets (e.g. commercially or contractually sensitive information) require more rigorous controls
- The most sensitive, High Risk assets (e.g. sensitive personal data, financial data) are protected by the most rigorous controls.

Exceptions

These Directives apply to all information handling whether on IT systems or on paper. However, it is recognised that some of the controls identified in Directives may be aspirational to a degree and full implementation will be achieved in due course.

Any exceptions to the ISMS Aspects Policies or associated Directives must follow the Security Exception Process; these must be reviewed and re-authorised at least annually.

Acceptable Use Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Acceptable Use Aspects Policy* which is defined in the *Aspects Policies*.

Please note that a number of statements in this Directive are replicated in the *Access Control Aspects Directive*, both of which are reviewed annually by employees. Care must be taken to ensure that any changes in this document are reflected in the *Access Control Aspects Directive*.

Objectives

To ensure that clear guidance is available relating to acceptable use of company assets and facilities.

Document Scope

This Directive applies to all information assets and facilities, including those relating to Company, customer and development assets across the Company.

Responsibilities

IT staff:	For ensuring that any technical controls within this Directive are effectively implemented.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Information Security assets and facilities.
Management:	Shall ensure their employees and contractors comply with this Directive.

General Principles

All Users are required to comply with all Information Security Policies and related Directives. Failure to comply may result in disciplinary action.

Confidential or sensitive information may only be transferred or stored outside of the Company on approved services.

Users must not attempt to access resources (internal or external), for which they have not been authorised.

Users are required to report any observed or suspected Information Security breaches or weaknesses in systems or services.

Users are not permitted to subscribe directly to external/cloud-based services without prior approval from the IT security team.

Users must use social media in a responsible manner, and not post any information that could be confidential in nature, or could be considered as be detrimental to the Company, in alignment with the Social Media Policy.

Users must not take any actions that circumvent any security technologies or controls that have been implemented.

Users must respect all legislation concerning intellectual property. Any used/installed applications or software must be appropriately licensed.

Personal Use

Information systems have been provided to conduct Company business. A limited amount of personal usage is permitted as long as the asset, or User, efficiency is not affected.

The following rules apply:

A limited usage of the messaging systems for personal needs is permitted as long as it is not to the detriment of professional activities.

No personal activities should take place on production or development infrastructure, including file storage, hosting or any other personal activities.

Personal emails and files must be identified as such and must be stored in a folder marked as 'Personal' or 'Private'.

Users must not use Company systems, technologies or infrastructure for personal gain.

Backup Policies have been implemented to protect work-related data. The Company is not responsible for backing up or any loss of personal information.

By entering into their contracts of employment, employees expressly acknowledge that any personal information that they reveal by using the Company's systems may be subject to the above scrutiny. Personal information is protected by the Company's obligations and duties under the Data Protection Act 2018.

Business Use

Email

The Company provides an email address to all employees as required for business operations. These resources are designed for business use. Messages sent or received are considered to be of professional content unless the personal nature is clearly indicated.

Any disclaimer or footer added to an email must not be deleted or modified in any way and must be used in all circumstances.

Email is not encrypted by default, so additional precautions such as file encryption must be used when confidential information is exchanged.

Users must:

- Not send or forward any message (including unsolicited spam) that contains illicit, offensive or discriminatory content
- Not redirect professional messages to an external personal messaging service
- Not open suspicious messages for which the origin, subject, or content are questionable (visible using the preview function) or for which they are not the normal addressee
- Delete files attached to suspicious messages without saving or executing these attached files
- Not send non-authorised communication of information concerning the Company activities or technology
- Not impersonate another person
- Inform the IT Security Team whenever a suspicious email is identified.

Internet Use

Where the Company provides Internet, a limited usage is permitted as long as it is not to the detriment of business activities.

Users must not engage in:

- Activities that jeopardise the legal responsibility of the Company or represent a threat to Company reputation
- Activities that consume a significant amount of Internet resources
- Attempting to access unauthorised external systems and/or resources
- Accessing Internet resources that are considered inappropriate, or illegal.

IT Equipment and Software

The Company provided IT equipment is configured to Company standards including hardware components, operating systems and software. This standardisation ensures the smooth running of operations within a secure environment.

If non-standard software is needed for business purpose, it will be installed upon request by the local IT support, with the approval of the User's manager.

Users must not attempt to modify their equipment configuration in any way and in particular they must not:

- Modify the hardware configuration of their equipment
- Add local Users to the system
- Reconfigure the software components installed on their computer, in particular modify security features, anti-malware software configuration, personal firewall software, remote connection software/VPN configuration or tracking or monitoring utilities
- Download non-approved applications.

Bring Your Own Device (BYOD)

Users of personal devices such as laptops, smartphones, tablets and external storage such as USB sticks or disks must:

- Take all necessary precautions to ensure the physical safekeeping of their equipment and avoid the risk of loss or theft.
- Respect the legislation in force concerning the use of and carrying of portable devices when traveling abroad
- Only use encrypted devices provided by the Company to store confidential information.

The loss or theft of personal devices could cause uncontrolled disclosure of confidential information. IT support or an Information Security Officer must be alerted immediately in case of loss or theft of these devices.

Clear Desk / Clear Screen

Users must lock/close their current working session, or log off, when leaving their computer system unattended.

At close of business on each day, Users must ensure paper, laptops, mobile devices, and removable storage media containing sensitive or confidential data are secured in a lockable cabinet or otherwise appropriately secured prior to leaving them unattended.

Acceptable Use Controls

In accordance with national regulations, the Company implements the necessary controls to ensure the security of its Information Systems, the protection of Users and third parties, and that Users conform to this Directive.

These controls can include the following elements:

- Restrict Internet access to websites with illegal content or that could have an adverse effect on the Company from a legal or operational perspective.
- Monitor Internet access for statistical and usage purposes.
- Tools to audit software packages and associated files installed on Users' computer equipment.

IT support monitors the use of software packages and may remove any non-standard software package not in regular use.

For troubleshooting purposes, IT support can take control of a User's workstation remotely. When possible, the User is informed prior to the action.

IT support may be required to open work-related messages or files. This access may occur at the request of the User's line manager.

Where non-compliance to this Directive is suspected, the User's line manager, the local Information Security Officer and/or the HR manager can request that personal messages, attached files or personal and private files are viewed.

Access Control Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Access Control Aspects Policy* which is defined in the *Aspects Policies*.

Please note that a number of statements in this document are replicated in the *Acceptable Use of Assets* document which has to be reviewed annually by employees. Care must be taken to ensure that any changes in this document are reflected in the *Acceptable Use of Assets* document.

Objectives

To ensure that appropriate consideration has been taken to ensure that Company and customer Information Assets are accessible by authorised persons only.

Document Scope

This Directive applies to all Information Assets, including company, customer and development across the Company.

Responsibilities

IT staff:	For ensuring that any technical controls within this Directive are effectively implemented.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Information Security Assets and facilities.
Management:	Shall ensure their employees and contractors comply with this Directive.

Network and System Access

Users may access Company networks and their own files by logging onto any PC on the system. However, access to network objects is limited by individual logins that are authorised on the basis of operational requirements.

Remote access to Company networks must be authorised on a least privilege basis, with access only granted to systems and resources where there is an explicit business requirement in compliance with the *Remote Working (Teleworking) Aspects Directive*.

Two-factor authentication (using an independent second factor such as SecureID, or digital certificates) must be implemented for access on all systems and network devices other than internal-only systems where this risk has been assessed and accepted.

Information Access

Access to information must be granted by the Information Owner on a least privilege basis.

Access to Confidential / Sensitive information must be reviewed at least annually.

Access to the email system will only be granted:

- If the User is an employee
- If the User is contractually engaged to perform a defined role in the Company and has an NDA when applicable.

Access to payment card data must be in compliance with PCI-DSS processes and procedures.

Data Access / User Accounts

All User accounts must be named according to a defined naming convention and must be uniquely identifiable using the assigned user ID/name.

User accounts must not be renamed, recycled or re-issued to another User.

All temporary and third-party accounts are permitted solely for the duration of the purpose they are required for.

Users must only be granted access rights in line with the access request and appropriate to their role. On a change of role, any historic access rights which are no longer relevant to the new role must be revoked prior to new access rights being granted.

Accounts of terminated staff must be suspended or disabled on leaving.

Privilege Management

All privileged access to Company systems or systems holding Company information must be approved through an appropriate approval procedure.

Access rights for privileged User IDs must be restricted to the minimum required for the user to carry out their business duties.

All privileged access accounts must be linked to a corresponding standard User account and to a verified individual User.

A standard User account must be used for all purposes not requiring privileged access.

Administrator accounts for applications or servers must only be granted to those Users who require such access to perform their job function.

The number of Administrators for each application or server must be restricted to the minimum required to support the system(s).

Administrative rights to client/desktop/laptop machines must only be granted to a limited number of Users and where there is a business need.

All administrative rights must be revoked once the business requirement has expired.

Access rights granted to privileged Users of information assets must be reviewed on an annual basis to ensure that they remain appropriate and to compare User functions with recorded accountability.

Administrator accounts on systems holding Confidential / Sensitive data must be controlled; their use must be logged, the logs must be regularly reviewed and any anomalies followed up.

Privileged access rights must be reviewed and re-approved on an annual basis.

Access to paper information

Documents labelled as Confidential / Sensitive and above must be restricted to authorised personnel only.

All documents have to be removed from desks outside of working hours and placed in locked cabinets or similarly protected areas.

All waste paper containing business information must be shredded.

Premises Security

Physical access to the premises and information systems is controlled in accordance with the *Physical Security Aspects Directive*.

Clear Screen

All computing devices must be locked with a secure password-protected screensaver or sessions logged off before being left unattended for a period of 5 minutes. This should support the practice of each User manually locking the device when leaving it unattended.

Password Usage

All passwords must be created in compliance with the Password Standards listed in Appendix A.

Passwords used for company applications/systems must not be used for personal applications/sites.

Passwords must be changed immediately should disclosure be suspected.

In the case of loss or theft of any physical authentication device such as a phone or token, the IT Security Team must be alerted immediately.

Appendix A: Password Protocols
Password Standards

Passwords must be sufficiently complex so as not to be easily guessed but should be easily remembered by the User. Passwords must comply with the following standards where technically feasible.

Passwords must be at least 12 characters in length.

Passwords must contain at least 3 of the following 4 categories:

- Upper case
- Lower case
- Number
- Special character e.g. # or ! etc.

Passwords are not routinely changed unless they are disclosed or there is a significant concern that a disclosure risk has or may have occurred. The exception to this is passwords providing access to high-sensitivity data where regular password changes are carried out for additional resilience.

Newly assigned passwords must be changed immediately to a unique password of the Users choosing, following the above protocol.

Asset Management & Disposal Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Asset Management & Disposal Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that effective asset management systems are in place and that appropriate consideration has been taken when disposing of assets such as Equipment (laptops, Desktops, Printers etc.) and Media (including USB connected hard drives and memory sticks). The disposal must take into account the type of information that resides on a particular devices/media to minimise the risk of data leakage.

Document Scope

This Directive applies to all information assets and facilities, including those relating to company, customer and development assets across the Company.

Responsibilities

IT staff:	For ensuring that technical controls relating to asset management and disposal detailed in this Directive are implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Information Security Assets.
Management:	Shall ensure their employees and contractors comply with this Directive.

Asset Management

Procedures and controls relating to acceptable use and management of assets are detailed in the *Acceptable Use of Assets Aspects Directive*.

Asset Disposal

Equipment is disposed of in alignment with local regulations including any approved donations/sales.

An asset disposal company is identified and contracted to provide this service (a third-party company that disposes of equipment taking into account local laws and environmental restrictions and can provide evidence of asset destruction).

Where the equipment containing company information is located at one of the hosting providers used for the company, the hosting provider is responsible for the secure disposal of equipment.

Laptops, desktops and company-owned mobile phones cannot be offered for sale or donation.

When a technical device has reached the end of useful life, or if the device is faulty, it must be returned to the IT department for processing. The following information must be removed:

- Company and/or client data
- The company licensed/configured system images
- Third-party software and licensing.

Some measures, such as physical media destruction, may not be applied to leased equipment. In these cases, other measures are taken to ensure that all practical steps are taken to erase data from the equipment. Equipment is evaluated to determine if it could contain information that would require any additional steps prior to return on lease.

Removable media is physically destroyed where practical, or sent to an authorised asset disposal company.

The disposal of equipment is recorded in the Asset Disposal Log and any assets are removed from the Information Assets Register.

Asset disposal companies disposing of equipment provide a certificate of disposal that uniquely identifies the asset. This certificate is retained for a minimum of three years.

Documents containing any information classified as 'restricted' or above are securely shredded.

Information Erasure

All information must be rendered unrecoverable and unreadable from equipment prior to leaving Company premises unless it is to an asset disposal company that contractually guarantees appropriate destruction of any information.

Equipment containing information that is considered as sensitive, or labelled as 'Confidential' such as personal information, credit card information, or commercially sensitive information is subject to erasure in a manner that makes data entirely unrecoverable.

The information which is stored on equipment that is hosted externally to the Company, i.e. with a cloud or dedicated hosting provider, is erased securely by the Company IT department.

Backup and Recovery Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Backup and Recovery Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate consideration has been taken to protect information from loss by the implementation of an appropriate backup strategy.

The core requirement is that a recent copy of all Information Assets is stored securely and is accessible to recover information in the event of non-availability of data assets. Note that this principle applies to cloud-hosted data assets where the backup is completed by the cloud service provider as a component of the cloud service provision with little or no local backup requirement.

Document Scope

This Directive applies to all information assets and facilities, including those relating to the company, customers and development assets across the company.

Responsibilities

IT staff:	For ensuring that backup, recovery and testing plans are implemented and records maintained.
Employees and contractors:	For ensuring that information is not stored in locations that are not included in the established backup protocols, such as local drives, USB sticks etc.
Management:	Shall ensure their employees and contractors comply with this Directive.

Backups

Spinwell Global do not host any business critical data on their own physical infrastructure or their own virtual infrastructure.

All business critical applications are provided by third party suppliers and delivered Software as a Service (SaaS).

All business critical SaaS suppliers undergo a robust onboarding process which includes an initial, and thereafter annual, review of their backup and business continuity policies.

Intermediate, non-critical working documents stored on company computing devices are automatically backed up to our primary file storage SaaS solution. This backup is not centrally monitored and is provided with best endeavours service levels. Employees are required to notify IT in the event there is an issue with this backup service.

Recovery

A plan is in place to test recovery from backup information to ensure that this meets the requirements of the Company and in accordance with the Business Continuity Plans.

Backup testing of all data assets is carried out at least annually according to the plan and the Company ensures that sufficient testing is carried out, in terms of frequency and quantity of test records restored, to maintain service levels agreed with the customer in the event of primary data asset loss.

A log is maintained of when recovery testing is carried out and the outcome.

Failure of any backup testing regime or individual backup restoration element is escalated to the IT Service Team and this results in a root cause analysis with subsequent changes to data asset storage procedures, backup protocols or both with the test plan updated accordingly.

Business Continuity Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Business Continuity Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to the company, customers and development assets across the company.

Responsibilities

IT staff:	For ensuring that the technical controls relating to business continuity detailed in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring all employees and contractors follow all controls relating to IT infrastructure operations and to highlight any concerns relating to operational issues and incidents.
Management:	Shall ensure their employees and contractors comply with this Directive.

Business Continuity - Principles

Business process owners are responsible for ensuring that the key events that can cause disruption to their processes are identified and that their potential adverse impact, financial and non-financial, is documented.

The scope of the Business Continuity Plan takes into account applicable factors including customer requirements and legal regulations. The following are considered while implementing any DR / BCP program:

- Identify critical business functions, applications and supporting technologies
- Develop an appropriate cost-effective recovery strategy
- Identify alternate, backup locations with the necessary infrastructure to support the recovery needs
- Identify the management and membership of the disaster response and recovery teams
- Identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan
- Train the recovery teams in the performance of their specific tasks
- Identify supplier recovery support capability
- Identify data protection and data recoverability status
- Identify functional team, recovery support and response capabilities
- Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

Business Continuity & Risk Assessment

A strategic plan, based on appropriate risk assessment, has been developed for the overall approach to business continuity. Key considerations in such a plan are:

- Identify events that cause interruptions to business processes
- Consider all critical business processes, not just information processing facilities.

Developing and Implementing Continuity Plans

All departments establish and use a logical framework for classifying all information resources by recovery priority that permits the most critical information resources to be recovered first.

All departments prepare, periodically update and regularly test the business recovery plan that specifies how alternative facilities are provided so employees can continue operations in the event of a business interruption.

Business Continuity Planning Framework

A single framework of business continuity plans is maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance.

Testing, Maintaining and Re-assessing Business Continuity Plans

If critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan will be developed, tested, periodically updated and integrated into computer and communication system contingency plans.

IT management annually revises and documents the support levels to be provided in the event of a disaster or emergency.

Computer and communication system contingency plans are routinely tested and followed up with a brief report to top management detailing the results.

On a quarterly basis, emergency contact information is validated and revised where required for every employee involved in business continuity and disaster recovery planning and implementation.

The roles and responsibilities for both information systems contingency planning and information systems recovery are reviewed and updated annually.

Cloud Computing Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Cloud Computing Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure all interactions with the cloud and cloud-based services do not represent an unacceptable risk to the company information security assets.

Document Scope

This Directive applies to all external cloud services, e.g. cloud-based e-mail, document storage, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), etc.

Responsibilities

IT staff:	For ensuring that the technical controls relating to business continuity detailed in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring all employees and contractors follow all controls relating to IT infrastructure operations and to highlight any concerns relating to operational issues and incidents.
Management:	Shall ensure their employees and contractors comply with this Directive.

Corporate Cloud Use

Use of cloud computing services for work purposes must be formally authorised by the ISMS Manager. The ISMS Manager will verify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing provider.

For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the ISMS Manager.

The use of such services must comply with the Company's existing Acceptable Use Aspects Directive.

Employees must not share log-in credentials with colleagues.

The use of cloud services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by the Company.

The ISMS Manager decides what data may or may not be stored in the Cloud and this is subject to periodic review.

Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

SSO and/or multi-factor authentication must be used where possible.

Cryptography Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Cryptography Aspects Policy*

which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate consideration has been given to protect the confidentiality, integrity and availability of data information by the implementation of an appropriate cryptography strategy.

Document Scope

This Directive applies to all information assets and facilities, including those relating to the Company, customers and development assets across the Company.

Responsibilities

IT staff:	For ensuring that the cryptography strategy is implemented and appropriate records maintained.
Employees and contractors:	For ensuring that full use is made of implemented cryptography systems in compliance with all requirements of this Directive.
Management:	Shall ensure their employees and contractors comply with this Directive.

Cryptographic Controls

Cryptographic controls must be implemented as required by the Information Classification Aspects Directive:

- Mandatory for information labelled as Sensitive
- Recommended for information labelled as Confidential.

Laptop hard drives must be whole-disk encrypted utilsing XTS-AES encryption with a 256-bit key.

All remote access is to take place via an encrypted VPN or an equally secure alternative.

All removable media containing company information, including memory sticks and external hard drives, must be encrypted.

WPA2 encryption must be used for all wireless networks carrying Company information.

Access to any web-based application must be encrypted using at least a 128-bit SSL certificate.

Email must be encrypted by using FIPS 140-2 encryption mechanism or similar whenever sensitive or critical data is included or attached.

Should a client request that sensitive or critical information be sent unencrypted, an indemnity opt-out letter (or e-mail) must be sent to the client before the transfer of data is made.

For any system storing payment card data, encryption must at a minimum be applied to render Primary Account Numbers (PANs - the long number on the front of the card) unreadable anywhere they are stored (including on portable digital media, backup media, in logs).

Regulation of Cryptographic Controls

Cryptographic security implemented on Company information systems must comply with local and international legislation including:

- Restrictions on import and export of computer hardware and software for performing cryptographic functions
- Restrictions on the usage of encryption
- Facilitation of access by countries' authorities to information encrypted by hardware or software.

Data Protection Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Data Protection Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that use of personal information is controlled in accordance with the Data Protection Act 2018 and General Data Protection Regulations principles and that an individual's rights are respected.

Document Scope

This Directive applies to all Information Assets, including those relating to Company, customer and development information across the Company and where personal data is processed by external providers.

Responsibilities

Data Protection Officer:	Responsible for reviewing the details of potential or actual breaches of personal data notifications to ensure that these are referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments. The Data Protection Officer has direct responsibility for DP procedures, including Subject Access Requests.
IT staff:	For ensuring that data protection controls are implemented and records maintained.
Employees and contractors:	For ensuring that data protection controls are followed and for notifying the Data Protection Officer of concerns or breaches of personally identifiable information (PII). All staff employed by the Company are also responsible for ensuring that any personal data that is about them that is supplied by them is accurate and up to date.
Management:	Shall ensure their employees and contractors comply with this Directive.

Data Protection Introduction

The Company needs to collect and use certain types of information about staff and other individuals who come into contact with the Company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material - and there are safeguards to ensure this is within the EU General Data Protection Regulation and the Data Protection Act.

A record of notification to the ICO is retained by the Data Protection Officer. The ICO Notification

Handbook is used as the authoritative guidance for notification. This notification is reviewed annually and update notifications are issued accordingly.

Any breach of the GDPR will be considered as a breach of the Disciplinary Policy and could also be considered a criminal offence, potentially resulting in prosecution.

Third parties working with or for the Company and who have or may have access to personal information will be expected to comply with this Directive. Third parties who require access to personal data will be required to sign a Confidentiality Agreement before access is permitted. This will also include an agreement that the company can audit compliance with the Confidentiality Agreement.

The company is a data controller and/or a data processor as defined under GDPR and the Data Protection Act 2018.

Data Protection Principles

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and company policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

Management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

All individuals are responsible for ensuring that any data held by the Company is accurate and up to date. Any data submitted by an individual to a Company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify the Company of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of the Company to ensure that any notification of changes to personal information is implemented.

The Data Protection Officer is responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

The Data Protection Officer will review, at least once a year, all the personal data processed by the Company, held in the Data Register. The Data Protection Officer will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of.

If a third party has provided inaccurate or out-of-date personal information, the Data Protection Officer is responsible for informing them that the personal information is inaccurate and/or out-of-date and will advise them that the information should no longer be used. The Data Protection Officer should also ensure that any correction to the personal information is passed on to the third party.

Personal Data

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and company measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

Compliance with this principle is contained in the Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001:2013 and the Security Policy set out in the ISMS.

Personal data shall not be transferred to a country or territory outside the European Union Member States unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

The transfer of personal data outside of the EU Member States is prohibited unless one or more of the specified safeguards or exceptions apply.

An assessment of the adequacy is carried out by the data controller, taking into account the following factors:

- The nature of the information being transferred
- The country or territory of the origin, and final destination, of the information
- How the information will be used and for how long
- The laws and practices of the country of the transferee, including relevant codes of practice and international obligations and
- The security measures that are to be taken as regards the data in the overseas location.

Accountability

The GDPR states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities and ensuring a Data Protection Officer is appointed, if required.

Data Subjects' Rights

Data subjects have the following rights regarding data processing and the data that is recorded about them:

- To make subject access requests regarding the nature of information held and to whom it has been disclosed
- To prevent processing likely to cause damage or distress
- To prevent processing for purposes of direct marketing
- To be informed about the mechanics of the automated decision-taking process that will significantly affect them
- Not to have significant decisions that will affect them taken solely by an automated process
- To sue for compensation if they suffer damage by any contravention of the GDPR

- To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
- To request the ICO to assess whether any provision of the GDPR has been contravened
- The right for personal data to be provided to them in a structured, commonly used and machine-readable format and the right to have that data transmitted to another controller
- The right to object to any automated profiling without consent
- Data subjects may make data access requests. These are reviewed by the Data Protection Officer and processed so that the procedure ensures that its response to the data access request complies with the requirements of the regulations.

Complaints

A Data Subject has the right to complain at any time to the Company if they have concerns about how their information is used. If they wish to lodge a complaint, this should be directed to the Data Protection Officer.

A Data Subject also has the option to complain directly to the Information Commissioner's Office. Details of the options for lodging a complaint should be provided.

Consent

'Consent' is taken by the Company to mean that agreement to the processing of personal data has been explicitly and freely given and that this consent is specific, informed and an unambiguous indication of the data subject's wishes. The consent of the data subject can be withdrawn at any time.

Consent is also taken by the Company on the basis that it has been given by the data subject who is fully informed of the intended processing and is in a fit state of mind and without undue pressure to give consent being applied.

There must be some active communication between the parties which demonstrates active consent. Consent cannot be inferred from non-response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely using standard consent documents. This may be through a contract of employment or during initial induction.

Data Security

Company staff that are responsible for any personal data must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised to receive that information and has entered into a confidentiality agreement.

Personal data should be accessible only to those who need to use it and access may only be granted in line with the Access Control Aspects Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

- In a lockable room with controlled access; and/or
- In a locked drawer or filing cabinet; and/or
- If computerised, it must be password protected in line with the *Access Control* and *Secure Systems & Development Aspects Directives*
- Stored on encrypted removable media in line with the *Cryptography Aspects Directive.*

Care must be taken to ensure that PC screens and terminals are not visible except to authorised staff. Staff must review the Acceptable Use Aspects Directive before they are given access to Company information.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit (written) authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving.

Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed. Because of the increased risk, all staff must be specifically authorised to process data off-site.

Data Access Rights

Data subjects have the right to access any personal data (i.e. data about them) which is held in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references and information obtained from third parties about that person.

Disclosure of Data

The Company ensures that personal data is not disclosed to unauthorised third parties including family members, friends, government bodies and, in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party. It is important to bear in mind whether or not a disclosure of the information is relevant to, and necessary for, the conduct of business operations.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

- To safeguard national security
- Prevention or detection of crime including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual - this refers to life and death situations.

Requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

Data Retention and Disposal

Personal data may not be retained for longer than it is required. Some data will be kept for longer periods than others.

Personal data must be disposed of in a way that protects the 'rights and freedoms' of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion, or obfuscation of personally identifiable data).

GDPR Risk Assessment

The Company needs to ensure that it is aware of any risks associated with the processing of all types of personal information. A Risk Assessment procedure has been implemented and is used by the Company to assess any risk to individuals during the processing of their personal information.

Assessments will also be completed for any processing that is undertaken on their behalf by any third-party organisation. Through the application of the Risk Assessment procedure, the Company ensures that any identified risks are managed appropriately to reduce the risk of non-compliance.

Where the processing of personal information may result in a high risk to the 'rights and freedoms' of natural persons, the Company will complete a data protection impact assessment, prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that the Company will process personal information in a manner that may cause damage and/or distress to the data subjects, the Data Protection Officer must review the process before the Company proceeds to process the information. If the Protection Officer decides that there are significant risks to the data subject they will escalate to the ICO for final guidance. The Company will apply selected controls for the ISO 27001 Annex A to reduce risk. This also references the Company's risk acceptance criteria and the requirements of the GDPR and The Data Protection Act 2018.

Human Resources Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Human Resources Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure all employees and contractors do not represent an unacceptable risk to the Company Information Security Assets.

To ensure that Users understand their responsibilities and are suitable for the roles they are considered for and to reduce the risk of theft, fraud or misuse of facilities.

Document Scope

This Directive applies to all information assets and facilities, including those relating to the Company, customers and development assets across the Company.

Responsibilities

Human Resources:	Responsible for ensuring that the employee life-cycle, (prior, during and at termination or change of employment) is managed without providing unacceptable risk to Company data assets and facilities.
IT staff:	For ensuring that the technical controls detailed in this Directive are implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Company Information Security Assets.
Management:	Shall ensure their employees, contractors and third-party Users: • Are qualified and understand their Information Security responsibilities • Are required to comply with all Information Security Policies and Directives • Ensure the Company termination process is implemented for employees • Return all assets on termination.

Prior to Employment

All screening and vetting procedures for potential employees and contractors must have been completed and be successful before a User is granted any access to the Company network and physical locations. These checks are detailed on an Induction Checklist and must include, as appropriate:

- Completeness and accuracy of the applicant's resume
- Confirmation of claimed academic and professional qualifications
- Independent identity verification
- Health Checks
- Right to work in the UK
- Criminal record check
- Financial probity check.

Background information shall be appropriately classified, labelled, handled, stored and destroyed in accordance with the *Information Classification Aspects Directive*.

Key elements of the Information Security policies must be reflected in contracts or terms and conditions of employment.

Contracts and agreements must include Company approved language relating to Information Security Policies.

Before being granted access rights, employees must confirm that they:

- Agree to comply with the Information Security Policies
- Understand that failure to comply with any part of their terms and conditions of employment, including those related to Information Security, can result in disciplinary action.

During Employment

The Company ensures that ongoing and appropriate IT security awareness and training programs are provided for employees so that they are trained adequately commensurate with their job functions and responsibilities. The awareness and training programs encompass standard and specific elements relating to job roles and responsibilities.
IT security awareness and training programs include but are not limited to the following aspects:

- Periodic IT security communications including but not limited to securing User ID and password management, acceptable use of Information Assets and personally identifiable information (PII), safeguarding sensitive data, changes in IT Policies/ procedures/Standards, reporting/handling policy violation, malicious software outbreak, etc.
- Awareness of cybersecurity threat and vulnerabilities and employee responsibilities including but not limited to:
    - Employees shall report any suspicious activity or security alerts (e.g. computer viruses) to IT support personnel and the Information Security Manager at the earliest opportunity
    - Employees are required to assist and comply with remedial instructions
- Interaction with, or handling, IT Systems and/or Information Assets
- Additional responsibilities for technical personnel.

Internet facilities are monitored for misuse and inappropriate use may be subject to disciplinary action. Employees shall note that in some legal jurisdictions, accessing certain prohibited sites is a criminal offence. As such, the Company shall report employees who access these sites, and in such circumstances, they may render themselves liable to prosecution. Employees shall not access sites

in Prohibited Categories which include, but are not limited to:

- All paedophile material and images including 'pseudo images'
- All pornographic related material
- Material promoting racism and/or sexism and/or discrimination of any kind
- Material promoting terrorist organisations and activities
- Computer hacking instructions and tools
- Any material that is likely to be reasonably considered by another employee to be of a grossly offensive, indecent, or depraved nature
- Material containing threats of violence of any sort
- Any material that can be reasonably construed as harassment or disparagement of others based on race, religion, national origin, sexual orientation, gender, age, disability, political belief or any other category prohibited by law.

All employees shall comply with all Security Policies and Directives at all times.

All Users must receive Information Security Awareness training as part of their induction or on-boarding process. This includes the incident reporting procedure.

All Users must receive regular updates and alerts on security issues as and when necessary, and that additional security-related training is made available as and when required.

Personnel with specialised security roles, e.g. IT teams, developers etc. must receive appropriate specialist training in line with their job requirements.

Termination of Employment

Human resource procedures are in place to manage, monitor and assign responsibility for termination or change of employment. A Leavers Checklist is used to manage this process and provide a record of completion.

All employees, contractors and third-party Users return all Company assets in their possession on termination of employment, contract or agreement. This includes, but is not limited to: software, computers, mobile devices, media, credit cards, access cards and tokens, ID badges and company information and documentation.

Management and Human Resources must be informed of the termination of a permanent employee to complete their employment records.

Access rights of employees, contractors and third-party Users to Company information, assets and facilities are removed on termination of employment, contract or agreement, or adjusted upon change of employment status (e.g. termination, leave of absence, administrative/gardening leave etc.) as appropriate.

On leaving the Company, the ex-employee is reminded of statements in his/her contract of employment relating to confidentiality and the Company's intellectual property rights.

Disciplinary Process

A disciplinary procedure is communicated and followed as the formal Disciplinary Policy for Company employees and third parties who have committed a breach of policies and directives. Further details can be found in the Company Employee Handbook.

Information Classification Aspects Directive

Purpose

To provide directives that support the Information Classification Aspects Policy defined in the Information Security Policies. These Directives are to ensure that information assets are protected and handled in an appropriate manner, proportionate to the risk.

Objectives

To ensure that information is appropriately classified, labelled and handled in a way that is appropriate to the sensitivity of the information.

Document Scope

This Directive applies to all types of information assets, including electronic or paper information, located on any media (removable or otherwise), and to any information held by third parties on behalf of the Company.

Responsibilities

Information Owner:	All information must have an information owner responsible for determining the appropriate classification, who can access the information, the appropriate controls to be used and managing any changes to the classification level that occur during the information lifecycle.
IT staff:	For ensuring that information classification controls detailed in this Directive are implemented and that records are maintained.
Employees and contractors:	For ensuring that information is not distributed beyond the intended recipient and/or user group and for reporting deviations and non-compliance to the information owner of the ISMS Manager.
Management:	Shall ensure their employees and contractors comply with this Directive.

Information Classification Principles

Where a document combines information of different levels or in case of doubt, the highest classification level applies.

As the classification level of a document may change over time (publications, press disclosure, etc.), assigned classification levels are reviewed regularly by the information owner and amended as appropriate.

All information is handled in a manner appropriate to its level of classification. Cryptographic technologies must be used to protect information, in transit or at rest, that is highly sensitive in nature, or mandated by its classification.

Third-party information will be treated as 'Internal Use' unless otherwise specified by the information owner. In particular, third-party information must not be forwarded to any other parties without the Information Owner's approval.

All information is labelled, usually within a document, and must fall into one of the categories listed in this Directive. If information is not explicitly labelled, then it can be considered to be classified as 'Internal Use'.

Classification and Handling

The following provides a summary of the information classification levels that have been adopted by the Company. These classification levels explicitly incorporate the Data Protection Act's 2018 (DPA) definitions of Personal Data and Sensitive Personal Data, as laid out in the Data Protection Aspects Policy.

Information Classifications Aspects Table

Classification	Description	Marking	Access/Recipients	Storage	Distribution	Copying	Disposal	Examples
Public	Information that has been approved by management for distribution outside the Company and may be broadly distributed without causing damage to the Company, its employees or stakeholders.	**'Public'**	Available to anyone	No specific instructions	Unlimited	Unlimited	Recycling/landfill	Press releases, advertising, job descriptions, general internet information.
Internal Use	This classification is for information that should not be distributed outside of the Company as it could be information that could give competitors an unfair advantage or damage the Company reputation. Unauthorised disclosure is not expected to very seriously or adversely impact the Company, its members, business partners and suppliers.	**'Internal Use' or no apparent marking**	Available to all employees and contractors who have signed a Non-disclosure Agreement when deemed necessary.	May be stored on electronic media such as backup tapes, CDs and DVDs or authorised cloud-based equivalent media.	External electronic – use encrypted transport media (USB drives etc.) Internal paper – not to be left on desks External paper – sealed envelopes	Copies may be made by employees or by contractors and third parties who have signed an appropriate non-disclosure agreement.	Hard drives, USB drives etc. – return to IT Support for secure disposal. Paper, CDs and DVDs – Secure disposal bins for secure shred.	Internal policies and directives, corporate strategies and plans, organisation charts, Company performance records.

	Note: This is the default information							
	classification for any information that has no stated classification or label.							
Restricted	This classification applies to less sensitive business information that is intended for distribution to a limited audience. Unauthorised disclosure could adversely impact the Company, its members, business partners and suppliers.	**'Restricted'**	Available to a limited list of authorised recipients, on a need-to-know basis	May be stored on electronic media such as backup tapes, CDs and DVDs or authorised cloud-based equivalent media. Paper and Media must be subject to secure store such as in a locked room/area. Encryption may be used where appropriate.	External electronic – encrypt when transiting networks, use encrypted media for data transport (USB drives etc.) Internal paper – not to be left on desks, use sealed envelopes. External paper – sealed envelopes, delivery by hand or signed-for delivery.	Limited copies may be made only with permission of the Information Owner.	Hard drives, USB drives etc. – return to IT Support for secure disposal. Paper, CDs and DVDs – Secure disposal bins for secure shred.	Employee performance records, operations data, audit reports.
Confidential	This classification applies to the most sensitive business	**'Confidential'**	Available to a very limited list of authorised	Not to be stored on removable	External electronic – encrypt	Limited individually numbered	Hard drives, USB drives etc. – return to IT	Financial data, personal

	information that is intended for use strictly within the Company. Its unauthorised disclosure could seriously impact the Company, its members, business partners and suppliers.		recipients on a need-to-know basis.	media, though encrypted removable media may be used to transport information only. The information must be encrypted when at rest. Paper and media must be subject to secure storage such as a locked room/area.	when transiting networks, use encrypted media for data transport (USB drives etc.) Internal paper – not to be left on desks, use sealed envelopes. External paper – sealed envelopes, delivery by hand or signed-for delivery.	copies may be made only when absolutely necessary with the permission of the Information Owner.	Support for secure disposal. Paper, CDs and DVDs – Secure disposal bins for secure shred.	data, corporate strategic plans, intellectual property.

Information Exchange Aspects Directive

Purpose

The purpose of this document is to provide Information Exchange directives that support the *Information Classification Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

The objective of this Directive is to establish a controlled environment that ensures:

- Information Exchange procedures are secured from unauthorised access, modification or theft
- Exchange agreements or contracts are in place that cover responsibilities and liabilities between the Company and external third parties
- Users are aware of their responsibilities when sending information to a third-party supplier or a client
- Incident management procedures are in place should any information be disclosed, lost or stolen whilst being sent to an external third party
- Information Exchange procedures comply with all legal and regulatory requirements.

Document Scope

This Directive applies to the following:

- Information assets including, but not limited to, client data, corporate data and employee data
- The external transfer of information via any electronic medium, e.g. e-mail, FTP/Secure FTP, secure website or portable storage device
- The external transfer of any physical copies of confidential information, e.g. Courier or Royal Mail
- All employees, contractors, temporary staff and external third-party suppliers who exchange/receive information.

Responsibilities

IT staff:	For ensuring that the technical controls detailed in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that Information Exchange is implemented in accordance with the information classification and exchange requirements detailed in these directives.
Management:	Shall ensure their employees and contractors comply with this Directive.

Information Exchange - Principles

Loss of data or any other incident suspected of impacting the secure external delivery of the company's confidential information should be reported to the ISMS Manager or the IT Helpdesk.

Incident management procedures are in place to ensure that any reported loss or theft of either electronic or physical data whilst in transit is appropriately managed.

Retention and disposal procedures are defined within exchange agreements or contracts to ensure data exchanged is disposed of in a secure and timely fashion and in accordance with all legal and regulatory requirements.

Liabilities for secure information exchange and secure processing of information are agreed and documented through contracts with the third parties prior to any exchange taking place.

Where a third party stores, processes or retains confidential data, a review of the third party's Information Security standards is carried out before the transfer occurs.

Information Classification

The Company operates an Information Classification scheme to identify information that must be controlled according to the classification level when being sent out of the Company. Refer to the Information Classification Aspects Directive.

Information Exchange

All electronic external data transfers involving confidential or restricted information are secured using industry-standard encryption techniques. The Company's corporate e-mail encryption solution is one such standard. Note: Password protecting a document such as Word, Excel or PowerPoint does not always provide sufficient protection.

Where confidential or restricted electronic data is sent via hardware, e.g. CD-ROM, USB device or tape drive, the device itself is encrypted. The device is sent by approved courier.

Passwords used to encrypt the information must be to a defined complexity protocol and comply with the requirements detailed in the Access Control Aspects Directive.

Passwords used to secure the information must be sent under a separate cover, e.g. by telephone/text and only divulged to the pre-agreed recipient of the information.

Procedures must be in place to confirm successful delivery or otherwise.

Unprotected confidential or restricted electronic information must never be sent over a public medium, such as the Internet.

Where appropriate, digital signatures should be used to ensure non-repudiation of electronic data transfers.

Emailing confidential information to a web-based e-mail system is strictly prohibited, even if using the corporate e-mail encryption solution.

If physical means are used to exchange information these must be carried by hand or sent using approved couriers or Royal Mail recorded delivery.

Malware and Vulnerability Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Malware and Vulnerability Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

The objective of this Directive is to protect the Confidentiality, Integrity and Availability of the Company's data assets and facilities by means of effective malware control measures to ensure effective technical vulnerability management.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to Company, customer and development assets across the Company and on all cloud environments utilised by the Company.

Responsibilities

IT staff:	For ensuring that the technical controls detailed in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that a vigilant and responsible contribution to the control of malware threats and technical vulnerabilities is made and for proactively reporting any concerns and/or incidents to the IT support team.
Management:	Shall ensure their employees and contractors comply with this Directive.

Malware and Mobile Code Protection

Anti-virus software is installed, configured and operational on all client and server systems.

Anti-virus software is regularly updated with current configuration and definitions. The anti-virus software automatically updates all client machines with new definition files within 12 hours of release.

Anti-virus software is configured to perform periodic scans. On production and other high-sensitivity systems, scans are scheduled to minimise operational impact.

Internet web traffic is scanned for malware and access to inappropriate content. Access to sites containing malware and inappropriate content is blocked and/or monitored.

Emails are scanned for malware and potential phishing threats. Suspicious email is quarantined with the recipient and the IT team is notified.

Technical Vulnerability Management

Systems and applications are patched in accordance with the vendor patching recommendations, with priority given to patches that may impact operational security. Systems that cannot be patched for any reason are subject to additional controls such as network isolation etc.

Devices connected to the Company networks are scanned for vulnerabilities on a regular basis at an interval determined by completion of the business risk assessment system.

All relevant new vulnerabilities must be communicated to the Technical Owner.

All vulnerabilities that are classified as high risk are remediated as soon as practical.

All other vulnerabilities must be subject to a risk assessment by the ISMS Manager in conjunction with any affected Information Owners to assess the potential impact to the Company and determine the remediation timeline and priority. Particular attention is given to vulnerabilities that may affect 'Restricted' information classification, and above.

Appropriate measures are taken within the agreed timeframe to mitigate the risk identified through the vulnerability investigation and risk assessment.

Any public facing systems are scanned for vulnerabilities on a continuous basis, with any newly discovered vulnerabilities being remediated in alignment with the identified business risk.

Employee Responsibilities

Inform the ISMS Manager immediately on receipt of a suspicious file or email attachment. Leave the attachment closed and await further instructions.

If required, macros are disabled whenever the relevant dialogue box appears, unless absolutely certain of the source of the document.

Save downloads to disk rather than opening them from a current location. This gives the malware system a better chance of detecting any malicious code.

Switch off any device that is suspected of being infected and ensure isolation from any network, and immediately inform the ISMS Manager.

Do not open any unexpected email attachments, even if the email appears to come from a known source.

Do not open an email attachment from an unknown or suspicious source, or one with a double extension, such as .file.txt.scr

Do not download any software or executable file whatsoever from the Internet without prior permission from the ISMS Manager.

The only exception to the above is the downloading of drivers or patches by an authorised member of the IT Support team or the ISMS Manager.

Do not flood the Company's system by passing on unconfirmed malware warning messages. The only malware warnings within the Company must come from the ISMS Manager.

Network Security and Network Systems Monitoring Aspects Directive

Purpose

The purpose of this document is to provide Network Security directives that support the *Network Security and Network Systems Monitoring Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate network security controls are implemented within the network and that the network infrastructure is appropriate to protect Company data assets and information.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to Company, customer and development network assets across the Company or externally with cloud/dedicated hosting providers.

Responsibilities

IT staff:	For ensuring that network security technical controls defined in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of network information security assets.
Management:	Shall ensure their employees and contractors comply with this Directive.

Network Security Directives - Principles

Trusted network ports should only be available in controlled areas where there is good physical security. In the event that there is poor physical security, such as in open office spaces that are shared with a third party, then additional mitigating controls must be implemented that limit access to only public facing interfaces and the absolute minimum connectivity into internal networks.

Note: There must be no unused active network ports connected to trusted networks in public areas, meeting rooms, training rooms or any other area where non-employees may be left unattended.

Only Company-owned and fully managed/supported devices may be connected to trusted networks.

The network administrator is alerted by the system if there is any possible breach of network security such as unauthorised access, hacking or malicious software infection.

Any devices that cannot be managed or patched (including 'Internet of Things' (IoT) devices), must be isolated on a separate untrusted network.

Only Company personnel are permitted to use devices connected to trusted networks. In the event that third parties such as clients or contractors are required to use Company devices connected to trusted networks, they must either be accompanied at all times, or have signed a formal confidentiality agreement.

Mobile phones, including those adhering to company standards, must only be connected to untrusted networks.

It is not permitted to directly connect a trusted network to any third party or cloud network with a VPN or any other WAN technology. Any requests to do so must be subject to a risk assessment process.

Changes to network configuration and firewall rules are implemented following change control procedures.

Firewall rules must be reviewed periodically for validity.

Any wireless infrastructure implementation must follow the Company standard.

Web servers accessible through the Internet are protected by an approved router or firewall.

There must be no ability to bridge traffic on a device between wired and wireless networks.

Network Logs

The following logs are compiled and retained:

- Network flows that cross company firewall perimeters
- Access to WiFi networks
- Access from remote access systems (VPN and non-VPN).

All logs are retained for at least 12 months. This logging includes the source IP/user and destination IP/URL and the user when this data is available.

All logs are protected from unauthorised access.

Network Flows

Where required, Company networks are segmented into areas of similar security requirements.

All equipment that is accessible from external networks is located on a service network. This equipment must be hardened with all unnecessary services removed or disabled.

All equipment is scanned for vulnerabilities prior to deployment and at regular intervals thereafter, and all high or medium rated risks are remediated.

No flows are permitted directly from external networks to trusted networks. A proxy device/relay located on a service network is used.

All flows between networks of differing security levels (trusted, untrusted and external) are limited to the minimum necessary to achieve the required function.

Traffic flows between the security levels listed below are not permitted without explicit authorisation:

- Flows from a less secure network to a more secure network such as external networks to untrusted networks, and untrusted networks to trusted networks
- Flows from trusted networks to external networks.

All trusted network access to the Internet uses a Secure Web Gateway to prevent access to malicious content and unauthorised websites. All other traffic is prohibited.

Cryptographic controls are implemented for traffic traversing external networks such as the Internet whenever practical. These controls used are implemented in alignment with the Cryptography Aspects Directive.

Network – Remote Access

VPN

Only Company personnel and approved third parties may use a VPN and only from approved Company supported and managed technologies.

A request for a VPN must be approved by the requestor's line manager and the ISMS Manager.

VPN connections must use multi-factor authentication, which may include at least two of the following; user credentials, certificates, biometrics, tokens, one-time passwords etc.

VPN connections will have direct access to trusted networks and resources.

VPNs must respect the rules defined in the Cryptography Aspects Directive.

Split tunnelling is not permitted; all network communication, including Internet access, must pass over the VPN to company networks once it has been established.

VPN access from third parties must implement controls that limit access to the necessary resources exclusively.

Non-VPN

Some applications may be published externally for access by authorised personnel from any device.

There is no requirement for multi-factor authentication: user credentials are sufficient as long as the rules relating to complexity and lifecycle are respected.

There must be no ability for information to pass directly from inside the Company perimeter to the connecting device such as file transfers and printing etc.

All communications are encrypted, following the rules defined in the Cryptography Aspects Directive.

Network Penetration Testing

In order to ensure that the Company network security systems remain effective, the Company or a delegated third party carries out periodic network penetration testing. The frequency of these tests is determined by the ISMS Manager based on event log and fault reports, etc.

Physical Security Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Physical Security Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate consideration has been taken with securing physical and environmental facilities to protect personnel and information security assets.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to the Company, customers and development assets across the Company.

Responsibilities

Building/Facilities Management:	For ensuring the security of the physical premises.
IT staff:	For ensuring that technical controls defined in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Company data assets and information.
Management:	Shall ensure their employees and contractors comply with this Directive.

Building Security - External

The Company utilises the services of cloud-based services from organisations that occupy suitable premises suitable for the purposes of the Company, taking into account environmental risks such as fire and flood.

All physical security perimeters are clearly defined. The siting and strength of each of the perimeters depend on the security requirements of the assets within the perimeter, as determined by risk assessment.

All perimeters of the building containing information, technology or other assets identified in a risk assessment are physically sound:

- The external walls of the site are of solid construction
- All doors and windows are locked when unattended
- Additional security protection for windows is considered where sensitive information and technology assets are being housed.

All external doors are alarmed, monitored by CCTV and suitably protected against unauthorised access with control mechanisms. CCTV footage is retained for at least six months or as prescribed by law.

The facility deploys 24/7 on-site security guards to provide cover out of normal working hours.

Any hazardous or combustible materials are stored at a safe distance from any information processing facility.

A Premises Security Checklist is completed by the Facilities Manager at least monthly to confirm that all premises security controls are in place and implemented.

Building Security - Internal

The Company utilises the services of cloud-based services from organisations that ensure that areas such as computer rooms, wiring closets, or any room containing sensitive equipment or information requiring additional protection have physical access controls including card readers or code locks to limit access to authorised persons.

The list of authorised persons to access each secure area is reviewed every six months and amended as required. Particular attention is given to the removal of access permissions where these have been previously granted for a limited, project-based purpose.

Secure internal areas are not to be used for purposes for which they were not intended, such as bulk storage of paper or other office supplies.

Equipment

Equipment used in a workstation desktop environment is sited to ensure that screen images are not visible to the outside public through windows.

Environmental conditions, such as temperature and humidity of information processing facilities are monitored to ensure that the conditions do not adversely affect the operation.

Cabling Security

Equipment used in a workstation desktop environment is sited to ensure that screen images are not visible to the outside public through windows.

Employee & Visitor Access

The Organisation operate a 'work from home' model currently, however, if the situation changes for operational purposes, where necessary, employees and visitors will be issued with identification (for example, a badge or access device) that will identify the visitors as non-employees.

All visitors will be required to:

- Sign a log to maintain a physical audit trail of visitor activity. The visitor's name, the firm represented and the employee authorising physical access will be recorded on the log. The log will be retained for a minimum of three months, unless otherwise restricted by law
- Return any identification that has been used for identification purposes before leaving the facility or at the date of expiry
- Return any issued access devices, such as key cards.

Remote Working (Teleworking) Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Remote Working (Teleworking) Aspects Policy* which is defined in the *Aspects Policies*.

Remote (Teleworking) is defined as working from a location that is not within the established Company environment or offices. This can include working from home, hotels, cafés, conferences etc.

Objectives

To ensure that access to data assets and information is adequately protected from unauthorised access, disclosure and/or theft when at locations that are outside of the normal working environment.

Document Scope

This Directive applies to all staff, contractors and third parties that require access to internal Company information from outside of the established environment/offices. This does not apply to customers accessing published Company information via online services.

Responsibilities

IT staff:	For ensuring that technical controls defined in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of company data assets and information.
Management:	Shall ensure their employees and contractors comply with this Directive.

Remote Working Principles

All Information Security Policies apply to persons accessing Company networks/internal resources via remote working/teleworking and mobile devices irrespective of location (in the office or outside of the established work environment). Particular attention must be given to the following:

- Complying with the Access Control Aspects Directive (complexity and sharing)
- Not sharing passwords with friends and family members
- Not leaving a device unlocked and unattended (Clear Screen Policy)
- Not allowing a family member or others to use Company access
- Anyone who suspects that there has been a breach of network security remote working must report it immediately to a member of IT Support Team.

Company information labelled 'Confidential' must not be transferred to personal systems. Non-'Confidential' information may be transferred as long as data confidentiality and integrity are preserved.

Company information must only be retained on personal devices for the minimum amount of time to meet the business needs.

Loss or theft of personal devices containing any Company information must be reported to the ISMS Manager.

Remote Working/Teleworking Directives

All personally owned laptops connecting to company networks must as a minimum:

- Be protected from unauthorised access by a PIN number and/or password and/or, fingerprint recognition (Touch ID), facial recognition or other recognised identification and authentication mechanism
- Have anti-virus software installed.

Only Company-supplied laptops are permitted to access the production environment from outside of the established Company network perimeter.

Non-company devices are permitted to access the non-production environment from outside of the established network perimeter.

Staff involved in software development connected to company networks and applications using VPNs and other secure technologies as appropriate. Other staff accessing company information and networks do so through secure web-based platforms using company devices.

Connecting to public WiFi hotspots, such as cafes, hotels etc. should be avoided where at all possible when accessing Company information or email. For these situations, a VPN should be used to protect from 'man in the middle' attacks.

Split tunnelling must be disabled on any device, (Company-owned or personal), when a VPN is established so that all traffic is routed via the VPN and not subject to break out locally.

Secure Systems & Development Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Secure Systems & Development Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate security controls are an integral part of any design or development lifecycle.

Document Scope

This Directive applies to all staff, contractors and third parties that require access to internal Company Information from outside of the established environment/offices. This does not apply to customers accessing published Company Information via online services.

Responsibilities

IT staff:	For ensuring that technical controls defined in this Directive are effectively implemented and records maintained.
Employees and contractors:	For ensuring that the controls in the Directive are followed to maintain the Confidentiality, Integrity and Availability of Company data assets and information.
Management:	Shall ensure their employees and contractors comply with this Directive.

Secure application environments

Applications must be designed to ensure that there is appropriate protection of information through the implementation of separate access layers. A typical architecture could implement a User Access layer, an Application Layer and a Data Layer.

Application layers must be implemented in separate network zones whenever possible in compliance with the *Network Security and Network Systems Monitoring Aspects Directive.*

All Operating Systems hosting applications should be built using the System Build Directives within this Directive.

Applications that handle or process cardholder data must be architected to comply with PCI Data Security Standards.

Security Incident Management Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Security Incident Management Aspects Policy* which is defined in the *Aspects Policies*.

'Incident' refers to any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service. The purpose of this Directive is to ensure that untoward events associated with information, information assets, physical security and other business/IT operations are communicated and managed in a manner allowing timely corrective action to be taken. The Directive establishes a consistent and effective approach to the management of incidents.

Objectives

The objectives of this Directive relating to the management of Information Security incidents are to ensure that:

1. Security incidents are reported and resolved in the minimum amount of time to mitigate their impact on the Company
2. Potential security incidents are prevented from happening in the first place
3. The Company's security is continually improved by the application of corrective and preventive action.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to Company, customer and development assets across the Company and on cloud and directly hosted environments.

Responsibilities

Incident Owner:	Accountable for overall management of the incident, including: • Ensures that all relevant stakeholders are informed/involved as necessary (via DPO) • Communicates with the Information Commissioner's Office where required • Ensures that the incident is managed in a timely and efficient manner.
IT staff:	For ensuring that the incident management technical controls defined in this Directive are effectively implemented and that records are maintained.
Employees and contractors:	For ensuring they are responsible for making a vigilant and responsible contribution to the security of the Company's information resources and reporting any concerns.
Management:	Shall ensure that their employees and contractors comply with this Directive.

Security Incident Principles

The Company has established a procedure for reporting any suspected incidents (security weaknesses or threats to information systems, premises or services etc.).

The details of the steps to be followed for reporting an incident are communicated to all employees and third-party contractors. Communication of the security incident reporting procedure is the responsibility of the respective department.

Users are made aware of their responsibilities in the event of a suspected security weakness such as the requirement that Users will not attempt to prove (or test) an identified security weakness. Such action on the part of Users is interpreted as a potential misuse of information systems and Users found doing so may be liable to disciplinary action.

Users are responsible for reporting any observed (or suspected) security weakness or any other incident immediately to the IT Department/Service Desk and will not share such information with internal or external parties.

Incident reporting and management procedures are made available for easy access and reference for the purpose of reporting of security incidents and weaknesses by Users.

Security Incident Management

Management responsibilities and procedures are in place to ensure a quick, effective and orderly response to security incidents.

The security incident management procedures ensure that:

- Different types of incidents are clearly defined and regularly updated, including:
    - Information system failure and loss of service
    - Distributed denial of service (DDOS)
    - Breaches of confidentiality and integrity
    - Unauthorised physical access or theft
    - Unauthorised access to the business premises
    - Misuse of information system.
- Analysis and identification of the cause of the incident are undertaken
- A record of the incident is made to provide the basis for subsequent review and corrective actions
- Guidelines are defined for categorising the incidents based on the severity of the incidents and their impact
- Corrective actions are defined based on the category of the incidents
- Planning and implementation of corrective action to prevent recurrence are carried out, if necessary
- Communication with those who are affected by or are involved in the recovery from the incident is completed
- An Escalation matrix is defined based on the category of the incidents
- Reporting the action is completed, where required, to the appropriate authority

- Audit trail and similar evidence are collected and secured
- Emergency actions taken are documented in detail, reported to management and reviewed. The action plan includes:
    - Particulars about the business unit or department
    - Facts and explanation/reasons for the incident
    - The severity of the incident
    - Other business units/departments affected
    - Corrective action to be taken
    - The estimated cost of implementing the corrective action (if any)
    - Estimated time frame, start date and end date.

Learning from Security Incidents

Reported incidents are stored and analysed on a regular basis to determine a common action plan to prevent recurrence of incidents.

Incident records are discussed at each Management Review at least annually or earlier based on the number and criticality of incidents.

Learning from the incidents is incorporated in Information Security Training and Awareness for employees.

Collection of Evidence

Formal procedures are in place to ensure adequate evidence is collected for the investigations involving security incidents.

Guidelines are defined to assess the admissibility and weight of the evidence based on applicable laws and published standards.

Social Networking Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Social Networking Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that clear information relating to use of social media is defined for employees and contractors to protect the reputation and goodwill of the Company.

Document Scope

This Directive applies to all social media platforms including:

- Blogs
- Online discussion forums
- Media sharing services, e.g. YouTube
- Social networking sites, e.g. Facebook, Twitter, Instagram, WhatsApp, Snapchat etc.

Responsibilities

IT staff:	For ensuring that the technical controls relating to social media, including monitoring, are effectively implemented and that records are maintained.
Employees and contractors:	For ensuring that the controls defined in this Directive are followed consistently and for reporting any concerns or breaches of this Directive.
Management:	Shall ensure their employees and contractors comply with this Directive.

Social Media Use - Principles

All employees should bear in mind that the information they publish via social networking applications is still subject to copyright and data protection legislation regardless of privacy settings.

Social networking applications must not be accessed during working time for personal use.

Reasonable access to social networking applications is permitted before and after working hours and during work breaks, provided this Policy is complied with in full.

Social Media – Publishing Information

Employees, both during and outside of working hours, must not use social networking applications to:

- Publish any information which is confidential to the Company, its customers/clients, employees or any third party
- Make or publish any critical, derogatory or defamatory statements about the Company, its customers/clients, employees or any third party
- Publish any content which may result in complaints or claims being pursued against the Company, including but not limited to claims relating to defamatory or discriminatory statements or breaches of copyright, Data Protection and confidentiality obligations
- Publish material of an illegal, sexual or offensive nature that may bring the Company into disrepute

- Breach the Company's Equal Opportunities Policy
- Bully and harass a colleague.

The use of company social media accounts is permitted for authorised activity such as advertising and sourcing suitable candidates. This could be through staff's personal social media profiles (e.g. LinkedIn) or through the company's official social media outlets.

Enforcement

Any breach of this Policy that causes damage to the reputation of the Company, its customers/clients, its employees or any third party or which brings the Company into disrepute will amount to either misconduct or gross misconduct (depending upon the seriousness of the breach) to which the Company's Disciplinary Procedure will apply.

In this Policy, a third party is defined as any other person or entity whom the Company has a relationship with such as a supplier, expert or consultant.

Supplier Relationship Aspects Directive

Purpose

The purpose of this document is to provide directives that support the *Supplier Relationship Aspects Policy* which is defined in the *Aspects Policies*.

Objectives

To ensure that appropriate controls are in place where the Company enters into a working relationship with a supplier or receives a third-party service.

Document Scope

This Directive applies to all Information Assets and facilities, including those relating to Company, customer and development assets across the Company and on cloud or directly hosted environments.

Responsibilities

IT staff:	For ensuring that the technical controls defined in this Directive are effectively implemented and records maintained.
Employees and contractors:	To ensure that only approved suppliers and contractors who have been suitably screened and/or verified are used to minimise the risk associated with external or third-party products and services.
Management:	Shall ensure that their employees and contractors comply with this Directive.

Supplier Relationship - Principles

Information Security requirements will vary according to the type of contractual relationship that exists with each supplier and the goods or services delivered.

The Information Security requirements and controls are formally documented

in a contractual agreement which may be part of, or an addendum to, the main commercial contract.

Separate Non-disclosure Agreements are used where a more specific level of control over confidentiality is required.

Supplier Relationship - Procedures

Appropriate due diligence is exercised in the selection and approval of new suppliers before contracts are agreed.

The Information Security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) are clearly understood and improved where necessary.

Remote access by suppliers is via approved methods that comply with Company Information Security Policies.

Access to Company information is limited where possible according to clear business need.

Basic Information Security principles such as least privilege, separation of duties and defence in depth are applied.

The supplier is expected to exercise adequate control over the Information Security Policies and procedures used by sub-contractors who play a part in the supply chain of delivery of goods or services.

The Company has the right to audit the Information Security practices of the supplier and, where appropriate, sub-contractors.

Incident management and contingency arrangements are put in place based on the results of a risk assessment.

Awareness training is carried out by both parties to the agreement, based on the defined processes and procedures.

The selection of required controls is based upon a comprehensive risk assessment taking into account Information Security requirements, the product or service to be supplied, its criticality to the Company and the capabilities of the supplier.

Cloud Services

Cloud service providers (CSPs) are clearly recognised as such so that the risks associated with the CSP's access to and management of Company cloud data may be managed appropriately.

Due Diligence

Before contracting with a supplier, it is incumbent on the Company to exercise care in reaching as full an understanding as possible of the Information Security approach and controls that the Company has in place. It is important that all reasonable and appropriate checks are made so that all of the required information is collected, and an informed assessment can then be made.

This is particularly important where cloud computing services are involved, as legal considerations regarding the location and storage of personal data must be

considered.

Addressing Security in Supplier Agreements

Once a potential supplier has been positively assessed, the Information Security requirements of the Company are reflected within the written contractual agreement entered into. This agreement takes into account the classification of any information that is to be processed by the supplier (including any required mapping between internal information classifications and those in use within the supplier), legal and regulatory requirements and any additional information security controls.

For cloud service contracts, Information Security roles and responsibilities must be clearly defined in areas such as backups, incident management, vulnerability assessment and cryptographic controls.

Appropriate legal advice must be obtained to ensure that contractual documentation is valid within the country or countries in which it is to be applied.

Suppliers that were not subject to Information Security due to diligence assessment prior to an agreement being made, are subject to an evaluation process to identify any required improvements.

Monitoring and Review of Supplier Services

In order to focus resources on the areas of greatest need, suppliers are categorised based on an assessment of their value to the Company.

Each supplier will be placed into one of the following four categories:

- Commodity
- Operational
- Tactical
- Strategic.

The recommended frequency of supplier review meetings between the Company and each supplier is determined by the supplier's category according to the following table:

Supplier Category	Meeting Frequency
Commodity	None
Operational	On Contract Renewal
Tactical	Annual
Strategic	Monthly/Quarterly

Each supplier has a designated contract manager within the Company who is responsible for arranging, chairing and documenting the reviews.

The performance of strategic suppliers is monitored on a regular basis in line with the recommended meeting frequency. This takes the form of a combination of supplier-provided reports against the contract and internally

produced reports.

Where possible, a frequent cross-check is made between the supplier reports and those created internally in order to make sure the two present a consistent picture of supplier performance. Both sets of reports are reviewed at supplier meetings and any required actions agreed.

Changes within Contracts

Changes to services provided by suppliers will be subject to the change management process. This process includes the requirement to assess any Information Security implications of changes so that the effectiveness of controls is maintained.

Contractual Disputes

In the event of a contractual dispute, the following initial guidelines must be followed:

- The Purchasing Manager must be informed that a dispute exists
- The Purchasing Manager will then decide on next steps, based on an assessment of the dispute
- Where applicable, legal advice should be obtained via the Managing Director
- All correspondence with the supplier in dispute must be in writing and with the approval of the Purchasing Manager
- An assessment of the risk to the Company should be carried out prior to escalating any dispute, and contingency plans put in place.

At all times the degree of risk to the business must be managed and minimised.

End of Contracts

The following process is followed for scheduled end-of-contract, the early end of contract or transfer of the contract to another party:

- The end of the contract is requested in writing within the agreed terms
- Transfer to another party is planned as a project and appropriate change control procedures are followed
- An assessment of the risk to the Company should be carried out prior to ending or transferring the contract, and contingency plans put in place
- Any budgetary implications are incorporated into the financial model.

The various aspects of ending a contract must be carefully considered at the initial contract negotiation time.

Amendment History

Version	Modified On	Modified By	Comments
0.1	06/09/2021	Chris Holden	Document created
0.2	08/09/2021	Chris Holden	
0.3	16/09/2021	Annabel Payne	
1.0	27/09/2021	Neil Dawes	
1.1	19/08/2022	Neil Dawes	Amended Acceptable usage directive and Data Access/User accoounts to reflect our working practices
1.2	24/08/2022	Neil Dawes	Amendments made to back up policy and cryptography
1.3	08/11/2022	Neil Dawes	Changed Password length to 12 characters