Renaissance Computer Services Ltd

Technology Standards

Document Reference: RCS-MIT-040

Version: 1.0

Effective Date: 1 April 2026

This document forms part of the Renaissance Managed IT Plans Agreement and sets out the minimum technology, security and operational standards applicable to systems forming part of a Customer's Managed Environment.

These standards are intended to support reliable service delivery, effective cyber security and the ongoing manageability of the Customer's technology environment.

The current version of this document is available through the Renaissance Contract Centre.

1. Purpose

This Technology Standards document forms part of the Agreement between Renaissance Computer Services Ltd ("Renaissance") and the Customer.

It defines the minimum technology, security and operational standards expected for systems forming part of the Customer's Managed Environment. These standards are intended to support the reliable, secure and efficient delivery of the Managed IT Plan and help ensure that the Customer's technology environment remains maintainable throughout the term of the Agreement.

The Technology Standards apply to all technology managed or supported by Renaissance under the Agreement, unless expressly stated otherwise within the Proposal or another Contract Document.

The standards contained within this document establish the minimum requirements for technologies supported by Renaissance. They do not prevent the Customer from implementing higher standards, additional security controls or more advanced technologies, provided these remain compatible with the Managed Environment and do not materially affect Renaissance's ability to deliver the Managed IT Plan.

Technology, cyber security threats and industry best practices continue to evolve. Accordingly, Renaissance may revise these Technology Standards from time to time in accordance with the Change Management provisions contained within the Managed IT Plans Terms & Conditions.

Where there is any inconsistency between this Technology Standards document and another document forming part of the Agreement, the Order of Precedence contained within the Managed IT Plans Terms & Conditions shall apply.

---

2. Application of the Technology Standards

These Technology Standards apply to the Customer's Managed Environment and are intended to establish a consistent baseline for the secure, reliable and effective operation of the Customer's technology environment.

The standards are intended to support the delivery of Renaissance's Managed IT Plans and assist in reducing operational risk, improving security, maintaining compatibility and promoting long-term technology resilience.

The applicability of individual standards will depend upon the scope of the services purchased by the Customer. Where a particular technology, system or service does not form part of the Customer's Managed IT Plan, Renaissance does not assume responsibility for its ongoing management, support or security. However, where that technology could reasonably affect the operation, security, performance or compliance of the Managed Environment, Renaissance may require that it meets the relevant Technology Standards or that appropriate compensating controls are implemented.

The Customer acknowledges that the overall security, resilience and compliance of the Managed Environment may be influenced by technology, systems or services that are not supplied or directly managed by Renaissance. Accordingly, Renaissance may make recommendations relating to any part of the Customer's technology environment where, in Renaissance's reasonable opinion, those recommendations are necessary to reduce operational or cyber security risk or to support the effective delivery of the Managed IT Plan.

Where technology does not comply with these Technology Standards, Renaissance will normally identify the non-compliance and make reasonable recommendations for remediation. The Customer will be expected to address the non-compliance, or demonstrate reasonable progress towards doing so, within twelve (12) months unless an alternative timescale is agreed in writing or the circumstances reasonably justify a longer period.

Where immediate compliance is not reasonably practicable, Renaissance may agree to continue providing services subject to one or more documented exceptions. Such exceptions may identify the affected technology, the nature of the non-compliance, the associated operational or cyber security risks, any agreed compensating controls and the Customer's acknowledgement of the residual risk.

Where technology remains materially non-compliant, Renaissance will continue to use reasonable endeavours to support the Customer wherever practicable. However, Renaissance reserves the right to:

- limit the scope of support provided for the affected technology;
- recommend the replacement, upgrade or reconfiguration of the technology;
- apply additional Charges where supporting non-compliant technology requires materially greater engineering effort; and
- exclude the technology from the Managed Environment where continued support would expose either Party to unreasonable operational, security or compliance risk.

Nothing within these Technology Standards prevents the Customer from implementing higher technical or security standards than those described in this document, provided such measures do not materially impair Renaissance's ability to deliver the Managed IT Plan.

---

3. General Principles

The Technology Standards contained within this document are intended to establish a consistent baseline for the management, support and security of the Customer's Managed Environment.

Unless expressly agreed otherwise in writing, technology forming part of the Managed Environment should comply with the following general principles.

3.1 Supported Technology

Technology should remain within the manufacturer's supported lifecycle and continue to receive security updates, firmware updates and vendor support where applicable.

Technology that has reached manufacturer end of support or is no longer capable of meeting the requirements of these Technology Standards may be considered non-compliant.

3.2 Security by Design

Systems should be configured in accordance with recognised security best practice and should support appropriate authentication, access control, encryption and security monitoring appropriate to their function.

Where reasonably practicable, security features provided by the manufacturer should be enabled and maintained.

3.3 Standardisation

The Customer should seek to minimise unnecessary variation in hardware, operating systems, software and cloud services.

Greater standardisation assists in improving reliability, reducing operational complexity and supporting more efficient service delivery.

3.4 Maintainability

Technology should be capable of being effectively monitored, maintained, updated and administered throughout its operational life.

Systems that cannot reasonably be managed using modern administration or monitoring techniques may require replacement or alternative management arrangements.

3.5 Licensing

All software, operating systems and cloud services should be appropriately licensed in accordance with the applicable vendor licensing terms.

The Customer remains responsible for ensuring that sufficient licences have been obtained unless Renaissance has expressly agreed to supply them.

3.6 Documentation

The Customer should provide, and Renaissance may maintain, sufficient technical information to support the efficient delivery of the Managed IT Plan.

Documentation may include asset records, supplier information, licensing information, configuration details and administrative contacts.

3.7 Business Continuity

Technology should be implemented in a manner appropriate to its business importance, taking reasonable account of resilience, recoverability and operational continuity.

The appropriate level of resilience will depend upon the Customer's operational requirements and the services purchased under the Agreement.

3.8 Continuous Improvement

Technology should be periodically reviewed to ensure it continues to meet current operational, security and business requirements.

Where Renaissance reasonably recommends improvements necessary to maintain compliance with these Technology Standards, the Customer should give due consideration to those recommendations and work towards implementation within a reasonable period.

---

4. Endpoint Standards

Endpoint devices form the foundation of the Customer's Managed Environment and are frequently the primary target for cyber security threats. Maintaining appropriate standards for endpoint devices helps improve reliability, security and the efficient delivery of the Managed IT Plan.

Unless expressly agreed otherwise, endpoint devices forming part of the Managed Environment should comply with the standards set out below.

4.1 Supported Operating Systems

Endpoint devices must run a manufacturer-supported operating system that continues to receive security updates and is suitable for business use.

Operating systems that have reached end of support, or which no longer receive security updates from the manufacturer, may be considered non-compliant.

4.2 Supported Hardware

Endpoint devices should be of sufficient specification, condition and performance to support:

- the installed operating system;
- current versions of business applications;
- modern security technologies;
- remote management;
- endpoint monitoring; and
- the effective delivery of the Managed IT Plan.

Where hardware no longer provides an acceptable level of reliability, performance or compatibility, Renaissance may recommend its replacement.

4.3 Manufacturer Support

Where reasonably practicable, endpoint devices should remain within the manufacturer's supported product lifecycle and continue to receive firmware, driver and hardware support.

Technology that is no longer supported by the manufacturer may present increased operational and cyber security risks and may be subject to the provisions relating to non-compliant technology.

4.4 Security Features

Endpoint devices should support, and where reasonably practicable have enabled, appropriate security technologies including:

- Secure Boot (or equivalent);

- hardware-backed security features, such as a Trusted Platform Module (TPM), where supported;
- full disk encryption where appropriate to the device and operating system;
- modern authentication mechanisms;
- endpoint protection software approved by Renaissance; and
- any other security controls reasonably required to support the Managed IT Plan.

4.5 Patch Management

Operating systems, firmware and supported applications should be maintained with current security updates.

The Customer shall not intentionally prevent or delay the installation of security updates where doing so would materially increase operational or cyber security risk, unless otherwise agreed with Renaissance.

Where updates cannot be applied due to application compatibility or other operational constraints, Renaissance may recommend alternative mitigations or compensating controls.

4.6 Endpoint Management

Where endpoint management forms part of the Customer's Managed IT Plan, supported endpoint devices must permit the installation and operation of the management, monitoring and security software reasonably required by Renaissance.

The Customer shall not knowingly remove, disable or interfere with such software without first consulting Renaissance.

4.7 Local Administrative Access

Local administrative privileges should be restricted to those Users who have a legitimate business requirement.

Where local administrative access is required, Renaissance may recommend appropriate controls to minimise operational and cyber security risk.

The Customer acknowledges that unrestricted local administrative access may increase the likelihood of malware infection, accidental system misconfiguration and unauthorised software installation.

4.8 Software Standards

Business applications installed on endpoint devices should:

- be appropriately licensed;
- remain within the vendor's supported lifecycle;
- receive appropriate security updates;
- be compatible with the supported operating system; and

- not materially impair the security or performance of the Managed Environment.

Renaissance may recommend the removal or replacement of software that no longer meets these standards.

4.9 Device Health

Endpoint devices should be maintained in a condition suitable for ongoing business use.

Devices demonstrating persistent hardware faults, storage failures, battery degradation, overheating or other reliability issues may be considered unsuitable for continued inclusion within the Managed Environment until appropriate remedial action has been taken.

4.10 Bring Your Own Device (BYOD)

Where personally owned devices are permitted to access the Customer's business systems, Renaissance may require appropriate technical and security controls before such devices are granted access to the Managed Environment.

Such controls may include device compliance policies, endpoint protection, encryption, multifactor authentication and remote management where appropriate.

The Customer remains responsible for ensuring that any BYOD arrangements comply with its own internal policies and any applicable legal or regulatory requirements.

---

5. Server Standards

Servers frequently host the Customer's critical business applications, data and identity services. Appropriate standards for server infrastructure help improve reliability, resilience, security and the effective delivery of the Managed IT Plan.

Unless expressly agreed otherwise, servers forming part of, or materially affecting, the Managed Environment should comply with the standards set out below.

5.1 Supported Operating Systems

Servers must operate using manufacturer-supported operating systems that continue to receive security updates and remain suitable for their intended purpose.

Operating systems that have reached end of support, or which no longer receive security updates, may be considered non-compliant.

5.2 Supported Hardware

Physical servers should be of sufficient specification, capacity and condition to support the workloads they host while maintaining acceptable levels of performance, resilience and reliability.

Where hardware no longer provides an acceptable level of operational reliability or compatibility, Renaissance may recommend replacement or upgrade.

5.3 Manufacturer Support

Where reasonably practicable, physical servers should remain within the manufacturer's supported product lifecycle and continue to receive firmware, driver and hardware support.

Where extended support arrangements exist, Renaissance may consider these when determining compliance with these Technology Standards.

5.4 Virtualisation

Where virtualisation is used, the underlying platform should be manufacturer-supported and configured in accordance with recognised industry best practice.

Virtual machines should be appropriately resourced and managed to support reliable operation and future growth.

5.5 Capacity and Performance

Servers should be appropriately sized to support their intended workloads, allowing sufficient processor, memory, storage and network capacity to maintain acceptable performance under normal operating conditions.

Where capacity constraints are identified, Renaissance may recommend appropriate upgrades or infrastructure improvements.

5.6 Security

Servers should be configured in accordance with recognised security best practice.

This should include, where reasonably practicable:

- current security updates;
- appropriate endpoint protection;
- secure administrative access;
- least privilege administration;
- supported encryption technologies where appropriate;
- logging and auditing appropriate to the server's role; and
- removal or disabling of unnecessary services.

5.7 Patch Management

Server operating systems, firmware and supported applications should be maintained with appropriate security updates.

Where updates cannot reasonably be applied because of application compatibility, operational requirements or vendor limitations, Renaissance may recommend alternative mitigations or compensating controls.

5.8 Monitoring and Management

Where server management forms part of the Customer's Managed IT Plan, supported servers must permit the installation and operation of the monitoring, management and security software reasonably required by Renaissance.

The Customer shall not knowingly remove, disable or interfere with such software without first consulting Renaissance.

5.9 Backup and Recovery

Servers hosting business-critical systems or data should be protected by backup arrangements appropriate to their operational importance.

Backup solutions should be regularly monitored and periodically tested to provide reasonable confidence that recovery can be achieved when required.

The Customer remains responsible for determining appropriate recovery objectives unless Renaissance has expressly agreed to provide business continuity or disaster recovery consultancy.

5.10 High Availability and Resilience

Where high availability or fault tolerance is required to support the Customer's business operations, appropriate technologies should be implemented having regard to the Customer's operational requirements and agreed service scope.

Such technologies may include:

- redundant hardware;
- virtualisation clustering;
- replicated storage;
- resilient networking;
- uninterruptible power supplies (UPS); and
- other resilience measures appropriate to the environment.

Unless expressly stated within the Proposal, Renaissance does not warrant that any particular server environment is fault tolerant or continuously available.

5.11 Physical Environment

Servers should be installed within an environment suitable for reliable operation.

This should include, where reasonably practicable:

- adequate ventilation;
- appropriate environmental conditions;
- protection from unauthorised physical access;
- stable electrical supply;
- surge protection; and
- appropriate power resilience for business-critical infrastructure.

---

6. Network & Connected Infrastructure Standards

The Customer's network provides the foundation upon which the Managed Environment operates. Network infrastructure and connected technology should be designed, implemented and maintained to support reliable operation, effective cyber security and appropriate resilience.

Unless expressly agreed otherwise, network infrastructure and connected technology that forms part of, or materially affects, the Managed Environment should comply with the standards set out below.

6.1 Network Infrastructure

Network infrastructure should be suitable for the operational requirements of the Customer and capable of supporting the services delivered across it.

This may include:

- firewalls;
- switches;
- wireless access points;
- routers;
- structured cabling;
- network controllers; and
- other infrastructure supporting business connectivity.

Infrastructure should be appropriately sized, maintained and configured to support current business requirements and anticipated operational growth.

6.2 Supported Equipment

Network equipment should remain within the manufacturer's supported lifecycle and continue to receive security updates, firmware updates and vendor support where applicable.

Equipment that has reached end of support may be considered non-compliant and Renaissance may recommend its replacement.

6.3 Secure Configuration

Network infrastructure should be configured in accordance with recognised security best practice.

Where reasonably practicable this should include:

- secure administrative access;
- current firmware;
- removal or disabling of unnecessary services;
- appropriate management protocols;
- secure authentication;
- encrypted administrative communications; and
- appropriate logging.

Default credentials should not be used on production systems.

6.4 Network Segmentation

Networks should be logically segmented where reasonably appropriate to reduce operational and cyber security risk.

Depending upon the Customer's environment, this may include separation of:

- business devices;
- servers;
- guest wireless;
- voice services;
- Internet of Things (IoT) devices;
- operational technology;
- CCTV;
- building management systems;
- access control systems; and
- other specialist equipment.

The extent of segmentation should be proportionate to the size, complexity and risk profile of the Managed Environment.

6.5 Internet Connectivity

Internet connectivity should be appropriate for the operational requirements of the Customer.

Where business-critical services depend upon internet connectivity, Renaissance may recommend additional resilience measures, including secondary connectivity or alternative failover arrangements.

6.6 Remote Access

Remote access to the Managed Environment should utilise secure technologies and appropriate authentication controls.

Where reasonably practicable, remote access should include:

- multifactor authentication;
- encrypted communications;
- appropriate access controls;
- logging of administrative access; and
- regular review of authorised users.

Renaissance may decline to support insecure remote access methods that no longer meet recognised security standards.

6.7 Connected Infrastructure

Technology connected to the Customer's network, whether or not directly managed by Renaissance, should be maintained in a manner that does not materially increase operational or cyber security risk.

This may include:

- CCTV systems;
- access control systems;
- intruder alarm systems;
- telephony platforms;
- audio-visual systems;
- printers and multifunction devices;
- environmental monitoring;
- manufacturing or industrial systems;
- specialist operational equipment;
- Internet of Things (IoT) devices; and
- other connected technology.

Where such technology could reasonably affect the Managed Environment, Renaissance may require reasonable information regarding its operation, connectivity and support arrangements.

6.8 Wireless Networks

Wireless networks should utilise appropriate encryption and authentication mechanisms consistent with recognised industry best practice.

Guest wireless services should, where reasonably practicable, be logically separated from business networks.

Wireless coverage, performance and resilience should be appropriate for the Customer's operational requirements.

6.9 Monitoring and Management

Where network management forms part of the Customer's Managed IT Plan, supported infrastructure should permit the installation and operation of the monitoring and management technologies reasonably required by Renaissance.

The Customer shall not knowingly disable, remove or interfere with such systems without first consulting Renaissance.

6.10 Documentation

Appropriate documentation should be maintained for network infrastructure and connected technology where reasonably necessary to support the Managed IT Plan.

This may include:

- network diagrams;
- IP addressing information;
- VLAN configuration;
- wireless configuration;
- administrative access details;
- supplier information;
- internet service details; and
- records of connected infrastructure.

---

7. Identity & Access Standards

Identity and access management plays a fundamental role in protecting the Customer's Managed Environment. Appropriate controls help reduce the risk of unauthorised access, data compromise and operational disruption.

Unless expressly agreed otherwise, identity services and access controls forming part of, or materially affecting, the Managed Environment should comply with the standards set out below.

7.1 Unique User Accounts

Each individual requiring access to the Managed Environment should be assigned their own unique user account.

Shared user accounts should be avoided except where they are technically necessary for specific systems or services.

Where shared or service accounts are required, appropriate controls should be implemented to minimise operational and cyber security risk.

7.2 Authentication

Authentication mechanisms should be appropriate to the sensitivity of the systems and information being protected.

Where reasonably practicable, authentication should support:

- modern authentication protocols;
- strong password policies;
- multifactor authentication;
- passwordless authentication where appropriate; and
- protection against common identity-based attacks.

7.3 Multifactor Authentication

Multifactor Authentication (MFA) should be enabled wherever supported by the relevant application, platform or service.

Where MFA cannot reasonably be implemented, Renaissance may recommend alternative controls or compensating measures to reduce the associated risk.

7.4 Privileged Access

Administrative privileges should be granted only where there is a legitimate business requirement.

Administrative accounts should, where reasonably practicable:

- be separate from day-to-day user accounts;
- be assigned to named individuals;
- be protected by Multifactor Authentication;
- be regularly reviewed; and
- only be used when administrative activities are being performed.

7.5 Least Privilege

Users should be granted the minimum level of access necessary to perform their normal duties.

Access permissions should be reviewed periodically and amended where operational responsibilities change.

7.6 Joiners, Movers and Leavers

The Customer should maintain appropriate processes to ensure that user accounts and access permissions are created, amended and removed in a timely manner.

This should include:

- creation of new user accounts;
- amendment of permissions following role changes;
- prompt removal or disabling of accounts when employment or engagement ends; and
- recovery of business-owned authentication devices where appropriate.

7.7 Service Accounts

Service accounts should only be used where technically necessary.

Where reasonably practicable, service accounts should:

- have clearly defined ownership;
- be appropriately documented;
- use strong authentication credentials;
- only be granted the permissions necessary for their intended purpose; and
- be periodically reviewed.

7.8 External Access

Access granted to third parties, suppliers, contractors or support providers should be restricted to the systems and resources necessary for their authorised activities.

Such access should be reviewed periodically and removed when no longer required.

7.9 Identity Monitoring

Where identity monitoring forms part of the Customer's Managed IT Plan, Renaissance may monitor identity-related events, authentication activity and other indicators of potential compromise using appropriate management and security technologies.

The scope of such monitoring will depend upon the services included within the Customer's Managed IT Plan.

7.10 Identity Providers

Where cloud-based identity services are used, they should be configured in accordance with recognised security best practice.

This may include, where reasonably practicable:

- protection of administrative accounts;
- secure authentication methods;
- conditional access or equivalent controls where supported;
- auditing and logging;
- recovery mechanisms for privileged access; and
- regular review of identity configuration.

7.11 Customer Responsibilities

The Customer remains responsible for ensuring that Users:

- keep authentication credentials confidential;
- promptly report suspected credential compromise;
- do not knowingly share passwords or authentication methods;
- comply with any security policies applicable to the Managed Environment; and
- cooperate with reasonable identity verification processes implemented by Renaissance.

---

8. Microsoft 365 & Cloud Service Standards

Cloud services frequently form a critical part of the Customer's Managed Environment. Appropriate configuration, administration and security controls help protect business information, improve operational resilience and support the effective delivery of the Managed IT Plan.

Unless expressly agreed otherwise, cloud services forming part of, or materially affecting, the Managed Environment should comply with the standards set out below.

8.1 Supported Services

Cloud services should remain within the provider's supported lifecycle and continue to receive vendor support and security updates where applicable.

Where a cloud service or subscription no longer provides the functionality or security capabilities reasonably required to support the Managed IT Plan, Renaissance may recommend migration to an alternative service or licensing level.

8.2 Tenant Administration

Cloud environments should be administered using recognised security best practice.

This should include, where reasonably practicable:

- named administrative accounts;
- separation of privileged and day-to-day accounts;
- appropriate role-based access;
- multifactor authentication for administrative accounts;
- regular review of administrative permissions; and
- recovery procedures for privileged access.

8.3 Licensing

Cloud service licensing should be appropriate to the Customer's operational, security and compliance requirements.

The Customer remains responsible for maintaining sufficient licences unless Renaissance has expressly agreed to supply and manage them under the Agreement.

Where licensing materially limits the availability of security features or management capabilities, Renaissance may recommend an alternative licensing model.

8.4 Security Configuration

Cloud services should be configured in accordance with recognised security best practice.

Where supported by the relevant platform, this may include:

- multifactor authentication;
- conditional access or equivalent access controls;
- protection of privileged accounts;
- security monitoring and alerting;
- audit logging;
- data protection controls; and
- appropriate configuration of security policies.

8.5 Email Services

Where email services form part of the Managed Environment, they should be configured to support reliable operation and appropriate cyber security.

This may include:

- spam and malware protection;
- email authentication technologies;
- secure mail flow;
- appropriate mailbox permissions;
- transport security; and
- protection against phishing and impersonation attacks.

8.6 Collaboration and Data Storage

Cloud-based collaboration platforms and data storage services should be configured to support appropriate security, availability and access control.

Where reasonably practicable, this should include:

- controlled external sharing;
- appropriate permissions management;
- version history where supported;
- audit capabilities;
- secure synchronisation; and
- protection against unauthorised access.

8.7 Domain and DNS Services

Where cloud services depend upon domain names or DNS services, those services should be appropriately managed and protected.

This may include:

- secure administrative access;
- appropriate DNS configuration;
- protection of domain registrar accounts;
- renewal management; and
- maintenance of accurate registration information.

8.8 Third-Party Cloud Applications

Applications integrated with the Managed Environment should be appropriately assessed before deployment.

Where reasonably practicable, consideration should be given to:

- vendor reputation;
- security capabilities;
- permissions requested;
- data protection implications;
- ongoing support arrangements; and
- compatibility with the Managed Environment.

Renaissance may recommend restricting or removing applications that present an unreasonable operational or cyber security risk.

8.9 Monitoring and Management

Where cloud service management forms part of the Customer's Managed IT Plan, supported cloud platforms must permit the monitoring, administration and security management reasonably required by Renaissance.

The Customer shall not knowingly remove, disable or interfere with management capabilities required for the effective delivery of the Managed IT Plan.

8.10 Business Continuity

Where cloud services support business-critical operations, the Customer should consider appropriate measures to protect against service disruption, accidental data loss and administrative error.

Such measures may include:

- appropriate backup solutions;
- retention policies;
- recovery procedures;
- resilience planning; and
- periodic review of recovery capabilities.

The Customer acknowledges that cloud platforms do not necessarily provide comprehensive backup or business continuity functionality as part of their standard service offering.

8.11 Platform Evolution

Cloud platforms evolve rapidly. Renaissance may recommend changes to licensing, configuration, security controls or service architecture where, in its reasonable opinion, such changes are necessary to maintain security, compatibility, compliance or the effective delivery of the Managed IT Plan.

---

9. Cyber Security Standards

Cyber security is a shared responsibility between Renaissance and the Customer. Appropriate technical controls, operational processes and user awareness are essential in reducing the risk of cyber security incidents and maintaining the security of the Managed Environment.

Unless expressly agreed otherwise, systems forming part of, or materially affecting, the Managed Environment should comply with the standards set out below.

9.1 Defence in Depth

The Managed Environment should utilise multiple complementary security controls designed to reduce the likelihood and impact of cyber security incidents.

Appropriate controls may include endpoint protection, identity protection, network security, email security, monitoring, vulnerability management and security awareness measures.

9.2 Endpoint Protection

Supported endpoint devices and servers should be protected by appropriate anti-malware technologies capable of providing real-time protection against known and emerging threats.

Where endpoint protection forms part of the Customer's Managed IT Plan, Renaissance may specify the security technologies used to deliver the service.

9.3 Threat Detection and Response

Where included within the Customer's Managed IT Plan, Renaissance may deploy technologies designed to identify, investigate and respond to suspected cyber security threats.

The scope of monitoring, investigation and response will depend upon the services purchased under the Agreement.

9.4 Vulnerability Management

Systems should be maintained in a manner that minimises known security vulnerabilities.

This should include, where reasonably practicable:

- timely application of security updates;
- removal of unsupported software;
- remediation of known security weaknesses;
- periodic review of system security; and
- implementation of appropriate compensating controls where remediation cannot immediately be completed.

Where Renaissance identifies significant vulnerabilities, the Customer will be expected to address them, or demonstrate reasonable progress towards doing so, within a reasonable period.

9.5 Email Security

Where email services form part of the Managed Environment, appropriate measures should be implemented to reduce the risk of phishing, malware, spoofing and other email-based threats.

This may include:

- anti-spam protection;
- malware scanning;
- email authentication technologies;
- attachment and link protection;
- user awareness measures; and
- appropriate mail flow configuration.

9.6 Security Monitoring

Where security monitoring forms part of the Customer's Managed IT Plan, Renaissance may monitor security events and indicators of compromise using appropriate technologies.

Monitoring activities may include:

- endpoint security events;
- authentication events;
- vulnerability alerts;
- suspicious activity;
- malicious software detection; and
- other events reasonably considered relevant to protecting the Managed Environment.

9.7 Security Awareness

Technology alone cannot eliminate cyber security risk.

The Customer should promote appropriate cyber security awareness amongst Users, including the recognition of phishing attempts, social engineering, password security and the prompt reporting of suspected security incidents.

Where security awareness services form part of the Managed IT Plan, Renaissance may assist the Customer in supporting these activities.

9.8 Security Incidents

The Customer shall notify Renaissance as soon as reasonably practicable upon becoming aware of any actual or suspected cyber security incident that could materially affect the Managed Environment.

The Customer shall provide reasonable cooperation during the investigation, containment and recovery of such incidents.

9.9 Security Recommendations

Renaissance may make recommendations intended to improve the security of the Managed Environment where, in its reasonable opinion, changes are necessary to reduce operational or cyber security risk.

Where recommendations relate to technology or services outside the scope of the Customer's Managed IT Plan, Renaissance will not assume responsibility for implementing or managing those recommendations unless separately agreed.

9.10 Compliance and Assurance

The Customer acknowledges that compliance with these Technology Standards contributes towards improving the overall security of the Managed Environment but does not guarantee protection against cyber security incidents or demonstrate compliance with any specific legal, regulatory or industry framework.

Where formal compliance, certification or assurance services are required, these must be separately agreed under the applicable Managed IT Plan or other commercial arrangement.

---

10. Backup & Business Continuity Standards

The loss or unavailability of business systems and data can have a significant operational impact. Appropriate backup, recovery and business continuity arrangements help improve organisational resilience and support the timely restoration of services following an incident.

Unless expressly agreed otherwise, systems containing business-critical information or supporting business-critical operations should comply with the standards set out below.

10.1 Business-Critical Systems

The Customer should identify the systems, applications and information that are important to the continued operation of the business.

Where business-critical systems have been identified, appropriate protection should be implemented having regard to the operational, financial and regulatory impact of their loss or unavailability.

10.2 Backup

Business-critical information should be protected by appropriate backup arrangements.

Backup solutions should be suitable for the importance of the protected data and should support recovery within timescales appropriate to the Customer's operational requirements.

The Customer remains responsible for determining the level of protection appropriate to its business unless Renaissance has expressly agreed to provide business continuity or disaster recovery consultancy.

10.3 Backup Security

Backup data should be protected against unauthorised access, corruption and loss.

Where reasonably practicable, backup arrangements should incorporate:

- encryption;
- secure storage;
- protection against accidental deletion;
- appropriate access controls;
- resilience against ransomware; and
- monitoring of backup operations.

10.4 Recovery Testing

Backup arrangements should be periodically tested to provide reasonable confidence that protected data and systems can be successfully restored.

The frequency and scope of testing should be proportionate to the operational importance of the systems concerned.

Where Renaissance provides managed backup services, testing may be included where specified within the applicable Service Schedule or Proposal.

10.5 Business Continuity

The Customer should maintain appropriate business continuity arrangements proportionate to the size and operational requirements of the organisation.

Such arrangements may include:

- documented recovery procedures;
- alternative working arrangements;
- communication plans;
- identification of critical business processes; and
- regular review of continuity arrangements.

10.6 Disaster Recovery

Where disaster recovery arrangements are implemented, they should be appropriate to the importance of the systems and services being protected.

Recovery arrangements should take account of:

- recovery priorities;
- system dependencies;
- infrastructure resilience;
- recovery procedures;
- restoration sequencing; and
- periodic validation of recovery capabilities.

10.7 Recovery Objectives

The Customer should determine appropriate Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for business-critical systems.

Unless expressly agreed in writing, Renaissance does not determine or guarantee any particular recovery objective.

Where Renaissance provides business continuity or disaster recovery consultancy, recommendations may be made regarding appropriate recovery objectives based on the Customer's stated business requirements.

10.8 Cloud Services

The Customer acknowledges that cloud platforms do not necessarily provide comprehensive backup, long-term retention or point-in-time recovery as part of their standard service offering.

Where appropriate, Renaissance may recommend additional backup or recovery solutions to provide protection against accidental deletion, malicious activity or administrative error.

10.9 Customer Responsibilities

The Customer remains responsible for:

- identifying business-critical information;
- determining acceptable business interruption;
- maintaining appropriate insurance where applicable;
- notifying Renaissance of material changes affecting recovery requirements; and
- reviewing recommendations relating to backup and business continuity.

10.10 Managed Backup Services

Where backup or disaster recovery services are provided by Renaissance under a Managed IT Plan or separate agreement, the scope of those services will be defined within the applicable Proposal, Service Schedule or Statement of Work.

Nothing within these Technology Standards should be interpreted as creating an obligation on Renaissance to provide backup, business continuity or disaster recovery services unless expressly agreed.

---

11. Operational Governance Standards

The ongoing management of the Managed Environment requires cooperation between Renaissance and the Customer. Effective governance supports reliable service delivery, continual improvement and the maintenance of an appropriate operational and security posture.

Unless expressly agreed otherwise, the Managed Environment should be managed in accordance with the standards set out below.

11.1 Shared Responsibility

The Customer and Renaissance each have responsibilities in maintaining the Managed Environment.

Renaissance will perform the services expressly included within the Customer's Managed IT Plan, whilst the Customer remains responsible for making timely operational and business decisions, providing information reasonably requested by Renaissance and implementing agreed actions that remain the Customer's responsibility.

11.2 Technology Lifecycle

Technology should be reviewed periodically to ensure that it continues to support the Customer's operational, security and business requirements.

Where equipment, software or services approach the end of their supported lifecycle, Renaissance may recommend replacement, upgrade or migration to maintain compliance with these Technology Standards.

11.3 Standards Compliance

The Customer should use reasonable endeavours to maintain compliance with these Technology Standards throughout the term of the Agreement.

Where non-compliant technology or practices are identified, Renaissance may recommend remedial action and agree a reasonable implementation timescale, taking into account operational priorities, business impact and commercial considerations.

11.4 Risk Management

Where the Customer elects not to implement recommendations made by Renaissance that are intended to address operational, security or compliance risks, Renaissance may document the associated risks and any agreed exceptions.

Such decisions shall not, of themselves, create any additional responsibility or liability on the part of Renaissance.

11.5 Change Management

Changes that may materially affect the Managed Environment should be planned and implemented in a controlled manner.

Where Renaissance is responsible for implementing changes, changes will be managed in accordance with its operational procedures and the applicable Managed IT Plan.

Where changes are implemented by the Customer or third parties, the Customer should notify Renaissance where such changes could reasonably affect the delivery of the Managed IT Plan.

11.6 Third-Party Suppliers

Where services are delivered by third-party suppliers, the Customer should provide Renaissance with reasonable cooperation and, where necessary, appropriate authority to liaise with those suppliers.

Renaissance will use reasonable endeavours to work collaboratively with third parties but cannot accept responsibility for services delivered by organisations outside its control.

11.7 Documentation

The Customer should notify Renaissance of material changes affecting the Managed Environment, including changes to infrastructure, business operations or key contacts, where those changes may affect the delivery of the Managed IT Plan.

Where documentation forms part of the Customer's Managed IT Plan, Renaissance will maintain documentation appropriate to the agreed scope of services.

11.8 Periodic Review

The Managed Environment should be reviewed periodically to identify opportunities for improvement, address emerging risks and ensure continued alignment with business requirements.

The frequency and scope of such reviews will depend upon the services included within the Customer's Managed IT Plan.

11.9 Continuous Improvement

Technology, cyber security threats and industry best practice continue to evolve.

Renaissance may make reasonable recommendations intended to improve the reliability, security, resilience or operational effectiveness of the Managed Environment.

The Customer acknowledges that maintaining an effective technology environment may require periodic investment in technology, licensing and services over time.

11.10 Review of Technology Standards

These Technology Standards are intended to evolve alongside technology, security best practice and Renaissance's service offerings.

Renaissance may amend these Technology Standards from time to time in accordance with the Agreement. The current version will be published in the Contract Centre and will apply from its stated effective date, subject to the provisions of the Agreement.