IT and Information Security Policy

Table of Contents

1 Purpose 4
2 Scope 4
3 Information Security Objectives 4
4 Policy Statement 5
5 Roles and Responsibilities 5
6 IT Information Security Compliance Management 5
7 IT and Information Security Risk Management 6
7.1 Aims of IT and Information Security Risk Management 6
7.2 Roles and responsibilities 6
7.3 Risk identification 6
7.4 Risk Assessment 6
7.5 Risk Treatment 7
8 Human Resources Security 8
8.1 Screening 8
8.2 Awareness and Training 8
9 Asset Management 8
9.1 Information Assets 8
9.2 Information Classification and Handling 8
9.3 Acceptable Use 8
10 Access Control 8
10.1 Formal Procedures for Allocating Access Privileges 9
10.2 Segregation of Duties 9
10.3 Use of Unique Accounts and Passwords 9
10.4 Allocation of Secret Authentication Information to Users 9
10.5 Password Management 10
10.6 Types of accounts 11
10.7 Access Logging and Monitoring 11
10.8 Review of and changes to Access Rights 11
11 Physical Security 12
12 Operations Security 12
12.1 Backup and Recovery Requirements 12
12.2 Change management 13
12.3 Malware Protection 14
12.4 Vulnerability and Patch Management 15
13 System Acquisition, Development and Maintenance 15
14 Supplier Relationships 15
15 Information Security Incidents 15
16 Business Continuity (BC) 15
17 Policy Review Date 16

Document Control

Document Control	
Title:	IT Information Security Policy
Reference:	IS-POL-020
Version:	0.1
Date:	27 January 2023
Status:	Final
Owner:	Product Director
Classification:	Internal

1 Purpose

The purpose of this policy is to define the objectives and requirements for IT and information security management within Triangle.

This policy is supported by a number of other policies referring to specific aspects of IT and information security.

Breaches of this policy may be dealt with under the Disciplinary Policy and, in serious cases, could be treated as gross misconduct leading to summary dismissal.

2 Scope

This policy applies to all Triangle staff irrespective of status, including temporary staff, contractors, consultants and third parties who have access to Triangle's data and systems. The scope of this policy includes, but is not limited to:

- All information processed by Triangle in pursuit of its operational activities, regardless of whether it is processed electronically or in paper form, including but not limited to:
    - External customer products, materials, information and reports;
    - Operational documents, plans, and minutes;
    - Financial and compliance records;
    - Employee records;
- All information processing facilities used in support of Triangle's operational activities to store, process and transmit information;
- All external organisations that provide services to Triangle in respect of information processing facilities.

3 Information Security Objectives

The IT and information security objectives of Triangle are the preservation of the **confidentiality**, **integrity** and **availability** of its information:

- **Confidentiality** – Protecting sensitive information from unauthorised disclosure, both to outsiders, and to employees or contractors who have no requirement to access such information in the course of their duties;
- **Integrity** – Safeguarding the accuracy and completeness of information and information processing methods, against any unauthorised changes;
- **Availability** – Ensuring that information and associated services are available to meet Triangle's business needs.

4 Policy Statement

Triangle's policy in regards to IT and information security is to ensure that:

- IT and Information security supports Triangle's business objectives;
- IT and Triangle's information security responsibilities are defined and communicated;
- IT Information security related policies, standards and procedures are in place to identify and mitigate IT and information security risks to an acceptable level, to protect Triangle's systems, infrastructure, and the information security requirements of interested parties, including the organisation's customers and business partners;
- The confidentiality, integrity and availability of Triangle's information and the places where that information is stored, handled and processed are maintained;
- IT and Information security risks to meet Triangle's business objectives are regularly identified and managed;
- In the event of a disruption, Triangle can continue to deliver an acceptable level of service of its critical activities to its interested parties;
- Appropriate information security requirements are included in contracts with third parties, where relevant;
- Triangle's information security related legal and regulatory requirements are met across all relevant jurisdictions;
- Triangle meets its customers' contractual information security obligations and provides assurance of its capability and capacity to manage information security adequately and meet its customer needs.

Compliance with this policy is mandatory to minimise business damage by preventing and minimising the impact of information security incidents. Such incidents can result in legal, regulatory or contractual breaches and financial or reputational loss to Triangle and/or its customers.

5 Roles and Responsibilities

- The Product Director is responsible for this policy and shall ensure that this policy is up-to-date and relevant.
- The Board is responsible for maintaining an up-to-date list of all legislative, statutory, regulatory and contractual requirements relevant for Triangle and its information systems.
- Line managers are responsible for ensuring that their staff comply with this policy.
- All authorised users shall adhere to this policy. Non-compliance shall be subject to investigation and may result in disciplinary action.

6 IT Information Security Compliance Management

Activities related to the use of Triangle's information including the systems and places where it is stored and processed shall be monitored to ensure that Triangle's requirements for confidentiality, integrity, and availability are maintained.

This policy is supported and supplemented by a number of IT and information security related policies(stored in a central repository and accessible to all relevant audiences:

- Triangle Acceptable Use of IT and Remote Working Policy
- Triangle Data Protection Policy

Compliance with applicable information security and data protection regulations shall be enforced, including European Union General Data Protection Regulation (GDPR) – see the Data Protection Policy.

Any deviation from this policy, or from any of Triangle's information security related policies, standards and procedures, shall be authorised by the Executive Board if, and only if, all of the following applies:

- A cost/benefit analysis of the available compliance options and risks of not complying has been performed, and clearly indicates that enforcing compliance would have an unacceptable business impact;
- Risk acceptance has been formally approved;
- Triangle remains compliant with legal and regulatory requirements.

7 IT and Information Security Risk Management

The policy of Triangle in regards to the management of information security risk is to identify, assess, treat, track, communicate and report all potential exposure to IT and information security risks. This is accomplished by embedding information security risk management into everything Triangle does.

7.1 Aims of IT and Information Security Risk Management

This policy aims to support these objectives by offering:

- Provisions for enhanced security measures for the protection of any customer, employee and/or business related data/information that Triangle handles;
- The introduction of conscious and balanced investment decision making in relation to information security risk mitigation (through a clear understanding of information security risk exposure and the costs and benefits of treatment options);
- The promotion of a proactive, information security risk aware culture across Triangle;
- Clear accountability and ownership for the management of information security risks across Triangle;
- A comprehensive understanding of Triangle's information security risk exposure, including any risks associated with third parties.

7.2 Roles and responsibilities

- Product Director is responsible for operating, maintaining and delivering continuous improvement to support information security risk management activities. This includes owning and keeping up to date this policy and the Risk Management Procedure; facilitating risk workshops to support the identification, assessment, mitigation, reporting and monitoring of risk, including management of the information security risk register; providing reporting on the management of information security risk to senior management; overall accountability for ensuring that information security risk is being managed in accordance with this policy.
- Senior Management shall be responsible for ensuring that this policy is followed and embedded within their areas of responsibility.
- It is the responsibility of all personnel in Triangle to ensure that they understand and adhere to this policy and the Risk Management Procedure.

7.3 Risk identification

It is the responsibility of all personnel to identify and raise information security risks where they are seen to exist within their respective business area.

All identified information security risks shall be recorded in the information security risk register, which shall be used to capture all the relevant information about each risk. The information security risk register shall be part of the corporate risk register.

7.4 Risk Assessment

All information security risks shall be assessed and evaluated in accordance with the below:

- A consistent approach to performing risk assessments shall be adopted, so that repeated information security risk assessments produce consistent, valid and comparable results;
- Information security risk criteria shall be established, including risk acceptance criteria;
- The information assets that need to be assessed, and the corresponding information asset owners, shall be identified;
- Relevant threats and vulnerabilities shall be identified;
- The impacts resulting from losses of confidentiality, integrity and availability shall be evaluated;
- The likelihood of threats exploiting vulnerabilities shall be evaluated;
- The resulting risk ratings shall be determined;
- Risk owners shall be identified;
- Risks ratings shall be compared with the risk criteria to determine whether risks shall be accepted or shall be treated;
- Risks which require risk treatment shall be prioritised.

7.5 Risk Treatment

Risk treatment is the process of selecting and implementing measures to manage the risk. The following requirements for risk treatment shall be met:

- Effective information security risk treatment options shall be evaluated and selected for risks that require treatment, based on the information from risk assessment.
- An information security risk treatment plan shall be formulated and include each risk to be treated; actions required; action owners; delivery dates; status per action;
- All security controls that are necessary to implement the selected information security risk treatment options shall be determined;
- Decisions to implement additional security controls per risk shall depend on a comparison of the risk value and the cost of control implementation;
- The residual risk value resulting from treatment of each risk, i.e. the risk remaining after the risk treatment has been implemented, shall be determined;
- The effectiveness of each selected control in lessening the risk shall be measured in terms of the residual risk;
- Risk owners' approval of the information security risk treatment plan and acceptance of the residual risks shall be obtained;
- Approval of the risk treatment plan and residual risks by the Information Security Risk Review Board shall be obtained;
- Where new controls are identified and implemented policies, procedures and/or standards shall be developed or updated, as relevant, to describe how these controls shall work in practice, and staff shall be made aware of their responsibilities, and trained where appropriate;
- In the event that necessary risk treatment cannot be implemented within budget or within the appropriate timeframe, the Company Board shall work with relevant information asset owners and control custodians to identify appropriate temporary mitigation and set appropriate timescales for necessary risk treatment, with decisions recorded;
- The Company Board shall ensure that the risk treatment plan is regularly reviewed and updated, with individual risks reviewed in accordance with the timescales below, depending on their risk rating - VERY HIGH=1 month; HIGH=3 months, MEDIUM=6 months, LOW/VERY LOW=12 months

8 Human Resources Security

8.1 Screening

Background verification checks on all candidates for employment shall be carried out in accordance with relevant regulations and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

8.2 Awareness and Training

Staff with access to Triangle's information, systems and the places where information is processed shall be educated on their information security responsibilities. Education shall be provided at induction so that new employees understand their responsibilities in respect of the protection of information and places where information is processed and stored.

Staff shall be provided with annual information security education and supporting reference materials as required by applicable regulations. Directors must ensure the provision of refresher courses and other related materials to regularly remind staff about their obligations with respect to information security.

9 Asset Management

9.1 Information Assets

Assets associated with information and information processing facilities shall be identified and an inventory of such assets will be maintained, with assigned owners.

9.2 Information Classification and Handling

Information shall be classified under an established scheme, to ensure that it is handled with an appropriate level of protection in accordance with its importance to Triangle – see the Information Classification and Handling Policy.

9.3 Acceptable Use

Rules for the acceptable use of assets associated with information and information processing facilities shall be identified, documented and implemented – see the Acceptable Use and Remote Working Policy.

10 Access Control

The policy of Triangle in regards to access control is as follows:

- Access to all Triangle data and systems shall be controlled and monitored;
- All access to systems and data shall be in accordance with the least privilege principle in that access is denied except where it is specifically required for functional purposes;
- Access to data or systems that are not in the public domain shall be subject to a confidentiality agreement either in a contract or as a condition of engagement;
- All system architecture, software and hardware shall be configured and controlled such that opportunities for unauthorised access or denial of service are minimised;
- All access procedures shall be fully documented;
- All users of information systems shall be authenticated and authorised. Authentication shall be, at a minimum, via the use of a password. For remote access, Multi-factor Authentication (MFA) shall be used, unless an exception has been approved by Information Security Management for instances where this policy cannot be applied (e.g. for legacy systems). MFA is not applicable to shared and/or service accounts (whether programmatic or individual person), but these accounts shall have additional compensating controls such as certificates and/or firewall policies to limit access;
- All users shall be accountable for their actions on Triangle systems.

- For any systems processing Highly Confidential data, access control effectiveness shall be tested and measured through a formal program of penetration testing. This shall be controlled by Triangle and shall be conducted by a trusted third party.

10.1 Formal Procedures for Allocating Access Privileges

- Access management processes shall be documented and implemented by providers of the systems/services and/or the business system owners.
- Access shall be granted to Triangle's IT networks and systems based on there being a business need for access. IT administrators and users shall only be provided with access to network services that they have been specifically authorised to use.
- All access privileges shall be assigned based on job classification, role and function. Access rights shall be restricted to the minimum necessary to perform a job role, based on a 'least privilege' principle.
- Access rights shall be controlled using pre-defined access profiles, based on job role and function.
- Access control mechanisms shall have a default 'deny-all' setting.
- All access requests, including new access requests and changes to access requests, shall only be granted where a formal request is raised and approved. Each documented approval shall list the specific privileges that have been approved.

10.2 Segregation of Duties

Authorisation and approval procedures shall ensure there is appropriate segregation of duties in place to reduce the risk of accidental or deliberate misuse of Triangle's information and information processing facilities.

In line with these requirements, the following shall apply:

- Access by business system managers and users shall be suitably restricted, e.g. with regards to financial applications;
- Access by IT administrators shall be restricted as far as possible;
- Access by software developers shall prevent them from accessing live systems without effective controls.

10.3 Use of Unique Accounts and Passwords

- Accounts shall not depict the purpose of the account login (e.g.: Backup, Admin).
- Accounts shall have application and technical owners who are responsible for the allocation and management of accounts and passwords.
- Access to information, systems and networks shall be controlled by the use of unique user accounts for both IT administrators and normal users. IT administrators shall use a unique IT administrator account for IT administration and a unique normal user account for all other work activities.
- Access shall only be allowed using a combination of a unique identifier and a unique password (or another unique authentication mechanism).
- Use of group, shared or generic user accounts shall not be permitted for IT administrator and normal user activities. All default, generic accounts shall be disabled or removed when feasible; otherwise the use of these accounts shall be blocked and prevented by strict access controls.

10.4 Allocation of Secret Authentication Information to Users

The allocation of secret authentication information, e.g. passwords, shall be controlled through a formal management process. The Managed IT Support Provider and business system owners shall ensure that the correct user is provided with the secret authentication information and that there is no risk of an unauthorised person obtaining the secret authentication information.

Access to information and information processing facilities shall be controlled. Users will only have access to the systems and services that they have been specifically authorised to use. Processes to grant and remove access, and to prevent unauthorized access to systems and applications, shall be applied.

10.5 Password Management

All IT administrators, business system owners and users shall comply with the following password management requirements[1]. These settings shall be enforced by network, system and application controls.

Password Settings	Detailed Requirements
Password complexity	Normal user accounts shall use passwords that are at least 8 characters in length. IT administrator accounts shall use passwords that are at least 14 characters in length. Passwords shall contain characters from three of the following four categories: • Uppercase characters (A through Z); • Lowercase characters (a through z); • Numbers (0 through 9); • Special characters (for example: !, $, #, %).
Password changes	Passwords shall be changed at least every 60 days. Privileged account passwords shall be changed every 30 days. The same applies to shared and generic accounts. Minimum age of a password shall be 5 days.
Password history	The last 12 passwords shall not be re-used.
Account lockout threshold and reset	A normal user account shall be locked out after 6 failed logon attempts. The lockout duration shall be at least 30 minutes or until an authorised IT administrator unlocks the account. An IT administrator account shall be locked out after 2 failed logon attempts until an authorised IT administrator unlocks the account.

There are also a number of additional password management requirements that shall be complied with as detailed below:

- Passwords shall be stored securely;
- Stored passwords shall be hashed using strong cryptography in line with current security industry best practice;
- Transmitted logon credentials shall be encrypted using strong cryptography in line with current security industry best practice;
- Logon procedures shall not display a password or password characters when it is being entered;
- If first time passwords are configured by IT administrators for users, then these passwords shall be unique per user and they shall need to be changed upon first logon. The same also applies for any password resets;
- Unsuccessful logons shall result in disconnection with no assistance. There shall not be any indication of which part of the logon data is in error, i.e. the user ID or password;
- A user's identity shall be verified before password resets are performed. Secure methods shall be implemented to ensure that remote users' identities are adequately verified;

[1] These requirements are aligned to the National Cyber Security Centre (NCSC) best practice guide to password management.

- Inactive sessions shall be terminated after a defined period of inactivity of no more than 15 minutes.

10.6 Types of accounts

Shared accounts

In certain circumstances it may be necessary and unavoidable due to business need or technical constraints for an account privilege to be shared amongst multiple users.

The business owner of the solution or service shall be the owner of any shared accounts and shared accounts shall be subject to periodic review.

Generic Accounts

Generic accounts may be required where a technology mandates a specific capability or naming for users or roles and shall only be used for specific business application needs.

There shall be a business owner of the solution or service for any generic accounts and they shall have additional controls and audit where MFA is not technically feasible;

Privileged Access Accounts

Privileged access accounts are those accounts such as Administrator, Maintenance and support accounts which have a higher level of privilege than the standard user account for a system or service.

There shall be a business and technical owner of the solution or service for any privileged accounts and their username and/or password shall be changed from the operating system (OS) or application default (e.g. Admin/Administrator);

They shall be auditable and recorded and they shall require an approved non-privileged account to increase privilege from. They shall use MFA for privileged access or prior to privilege escalation.

Third Party Support Accounts

Third party support accounts are those accounts for partners and suppliers to access specific Triangle systems or services. Where technically feasible they shall be disabled when not in use; they shall have MFA and there shall be a business owner of the solution or service for any third party support accounts.

10.7 Access Logging and Monitoring

All access events relating to any Triangle networks, systems and applications shall be logged and regularly monitored.

10.8 Review of and changes to Access Rights

All access privileges shall be subject to regular review on a quarterly basis, including access to networks, operating systems, applications, services and software. The IT Department shall review access in line with this requirement, whilst business system owners shall specifically review access to the systems that they are responsible for.

Whenever temporary access is granted, the access shall be revoked within a formally defined time period.

All changes to access rights shall only be granted where a formal request is raised and approved. Each documented approval shall list the specific privileges that have been approved, and / or those that have been revoked.

The Managed IT Support Provider and business system owners shall ensure that user accounts are deactivated after 90 days of inactivity.

Line managers shall ensure that the Managed IT Support Provider and all relevant business system owners are notified of any requirements for revoking access rights, e.g. when an employee moves within or leaves Triangle, in accordance with the Movers, Joiners and Leavers Procedure.

When an employee leaves Triangle, the line manager shall be responsible for ensuring that all Triangle assets, such as PCs, laptops, mobile phones and physical security access devices / badges are returned to Triangle.

11 Physical Security

Security measures shall be applied to:

- Prevent unauthorized physical access, damage and interference to Triangle's information and information processing facilities;
- Prevent loss, damage, theft or compromise of assets and interruption to Triangle's operations.

For Triangle offices, doors and windows shall be locked when unattended and external protection shall be considered for windows, particularly at ground level. Access to each site shall be restricted to authorised personnel.

For data centres processing Triangle data and supporting Triangle's systems, secure and safe physical environments will be covered by the contractual agreements in place.

See the Acceptable Use and Remote Working Policy for more detail on physical security outside of Triangle's offices or contracted physical environments.

12 Operations Security

Processes and mechanisms shall be in place to:

- Ensure correct and secure operations of information processing facilities;
- Ensure that information and information processing facilities are protected against malware;
- Protect Triangle against loss of data;
- Record events and generate evidence;
- Ensure the integrity of operational systems;
- Prevent exploitation of technical vulnerabilities.

12.1 Backup and Recovery Requirements

Business system owners shall define requirements for information backups, on a per information system basis, via formal business impact assessments. In this way, the criticality of the information shall be determined, which in turn shall dictate the requirements for backup, retention and recovery in terms of:

- What needs to be backed up;
- The frequency of backup, e.g. daily or weekly;
- Whether full or partial backups, or snapshots, are needed;
- Whether encryption of backups is required, i.e. for the secure storage of sensitive information such as personal or commercial information;
- Secure storage and availability to authorised individuals of encryption passphrases or certificates/key data for recovery from backup onto newly installed resources if required;
- The period of time the information needs to be retained
- The Recovery Time Objective (RTO);
- The Recovery Point Objective (RPO).

The Managed IT Support Provider shall identify, implement and maintain suitable backup and recovery solutions for Triangle's electronic information, software and systems. By default, all backups shall be made to a storage repository with robust security controls, which protect the backup copies. The adequacy of the backup and recovery solutions shall be reviewed on at least an annual basis.

All critical systems shall be backed up on at least a daily basis. Backups for critical systems shall be formally scheduled to run at the most appropriate time, e.g. a quiet processing time outside of normal operating hours.

All critical cloud-based services for which Triangle is responsible for backup and recovery shall be backed up / have recoverable image snapshots taken on at least a daily basis. These backups shall be formally scheduled to run at the most appropriate time, i.e. a quiet processing time outside of normal operating hours.

All critical systems / services shall be backed up / have a snapshot taken at an appropriate point before any significant / major new deployment, to support rollback in the event of issues with deployment or operation of new versions of system or service.

All infrastructure configuration if not backed up as part of the requirements above shall be securely backed up and stored.

Accurate and complete records of the backup copies shall be maintained, and inventory records shall be reviewed at least annually.

Operational processes shall monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups. The Managed IT Support Provider shall ensure that suitable alerting and response facilities are in place.

The backups shall be stored in remote locations, at a sufficient distance to escape any damage from a disaster at the site which hosts the systems that are backed up.

The security of off-site storage locations shall be reviewed at least annually. Backups shall be given an appropriate level of physical and environmental protection consistent with the standards applied to the source information.

The transportation of backups and where backups are located shall be logged within backup media inventories. The transport of all backup media shall be authorised by management, and sent via secure courier services or other delivery method that can be tracked.

Documented recovery procedures and recovery testing schedules shall be maintained and exercised by the Managed IT Support Provider and relevant business system owners.

Where specific hardware is required to recover backups, availability and compatibility of said equipment shall be validated on an annual basis. Where systems or services involving Triangle information are delivered by cloud providers, they shall include backup and recovery capabilities in line with this policy.

12.2 Change management

Change management is a critical component to healthy and sustainable IT systems and infrastructure.

There must be a robust process for requesting, evaluating, testing, and implementing changes to prevent an adverse impact to the existing IT network and systems, and all changes must be subject to authorised approval.

All changes shall be assessed based on their urgency, impact, benefit and risk while providing the appropriate stakeholders the authority to approve or decline the request accordingly and all changes are logged and captured in a centralised documentation where the information can be shared, retrieved and reported on.

There shall be timely communication of change implementation plans and schedules, availability of appropriate resources and consideration of other changes being deployed.

Roles for change management process:

- Change Requester - providing detailed description of the change and all associated information, doing the initial assignment of the type of change; Knowing what changes they are authorised to request, and obtaining authorisation to request them when required; Participating in and providing input to a post-implementation review if required.
- Technical Lead – reviewing the request and preparing an implementation plan, including a risk assessment, testing plan and rollback plan; Participating in and providing input to a post-implementation review if required.
- Change Implementer – have overall responsibility for the implementation of the change (once approved), including reviewing the documented outcomes of testing and operational readiness activities for the change; implementing the rollback plan for the change if unsuccessful; or, if not, raising an IT incident for resolution; Participating in and providing input to a post implementation review if required.

- Change Manager – ongoing overall oversight of change requests, implementations and the change management policy – leads on post implementation reviews where required.

The category of a change determines the level of rigor required for evaluating, approving and implementing it. All changes will be classified in one of the following categories:

- Standard changes correspond to specific types of low risk changes that follow an accepted and established procedure or work instruction and are pre-approved by the Change Manager;
- Emergency changes that are required to quickly restore service or prevent service disruption in exceptional circumstances. For this reason, they follow a less strict process of approval and implementation;
- Normal changes that are neither standard nor emergency changes. They follow the full process of change approval and implementation.

All CRs will be prioritised based on the urgency and impact of the change, as well as their relation to other scheduled or pending CRs. Specific circumstances may also affect priority such as disasters, regulatory compliance, etc. Priority is used when two changes are in conflict. The change with the higher priority will always take precedence.

12.3 Malware Protection

- Information Security – and third parties who provide malware protection services to Triangle – shall monitor security industry recognised sources of information concerning the latest malware threats and vulnerabilities.
- Triangle shall implement central controls that prevent (blacklist) the use of known or suspected malicious websites associated with malware distribution.
- Central controls shall also be implemented to scan inbound and outbound e-mails for malware, at any corporate e-mail ingress/egress. If inbound encrypted e-mail cannot be scanned, it shall be quarantined, and the intended recipient shall be informed, and given the opportunity to request release of the e-mail from its quarantine.
- Approved anti-malware software shall be deployed with on-access scanning on all systems commonly affected by malicious software, e.g. personal computers, laptops and servers with commonly affected operating systems.
- Deployed anti-malware software shall be capable of detecting, removing, and protecting against all known types of malicious software. Examples of types of malicious software include viruses, worms, Trojans, spyware, adware, and rootkits.
- Deployed anti-malware software shall be capable of identifying behaviours which are indicative of malware and be able to reliably alert to the risk of previously unseen or “zero-day” malicious code which could represent a risk to Triangle.
- All anti-malware mechanisms shall be maintained as follows:
    - Anti-malware software and definitions / methods shall be kept up to date on a daily basis;
    - As new capabilities are added to the anti-malware software, they shall be assessed and enabled for endpoint computers and, where technically feasible, servers/services;
    - Computer devices used by mobile and home workers shall be updated from approved sources regardless of location; remote alerting and logging shall be enabled;
    - In the case of client devices such as PCs and laptops, all accessed files shall be scanned at the time of access; in the case of servers, real-time, on-demand scans of files shall take place, as well as full disk scans on a weekly basis;
- Anti-malware mechanisms shall be actively running and shall not be disabled or altered by users, unless specifically authorised by management on a case-by-case basis for a limited time period. Additional security measures shall be implemented for the period of time during which anti-malware protection is not active, e.g. restricted e-mail and Internet usage.
- Files found to be affected by malicious software shall be quarantined or securely removed.

- Procedures shall be defined to deal with recovering from malware attacks. Appropriate business continuity plans shall be prepared for recovering from malware attacks, including all necessary data and software backup and recovery arrangements.
- Malware protection services may be provided by third parties under contractual agreements.

12.4 Vulnerability and Patch Management

- Triangle shall regularly monitor vulnerability and security patch information published by vendors and other recognised security industry sources;
- Vulnerabilities shall be identified and managed using a formal, regular programme of vulnerability scanning and penetration testing, supported by appropriate tooling and including testing by trusted third parties;
- The implementation of software security patches shall be managed in a structured and controlled way to ensure that Triangle is constantly protected against the impact of software vulnerabilities;
- Patches shall be applied within timeframes commensurate to the vulnerability risk level and the relevance and data classification of the impacted systems and data.

13 System Acquisition, Development and Maintenance

Processes and mechanisms shall be in place to ensure that information security is an integral part of information systems across the entire lifecycle, irrespective of whether they are provided by third parties or developed internally. Changes to systems including acquisition will be handled through the Change Management policy set out above.

14 Supplier Relationships

Processes shall be in place to ensure protection of Triangle's information that is accessible by suppliers. Information security requirements, aligned to Triangle's information security related policies, shall be incorporated in contracts with the relevant suppliers. Agreed levels of information security and service delivery shall be maintained, in line with supplier contracts.

15 Information Security Incidents

See the Information Security Incident Response Policy for more detail.

16 Business Continuity (BC)

Information security continuity shall be embedded in Triangle's business continuity management system. A managed process has been developed and maintained for BC management in Triangle. This incorporates the following key elements:

- Ensuring the safety of personnel and the protection of information processing facilities and organisational property;
- Ensuring all relevant areas are considered, including, but not limited to, interested parties and their requirements and legal and regulatory requirements;
- Identifying all critical business processes;
- Identifying all the assets involved in critical business processes;
- Understanding the risks, in terms of likelihood and impact, related to critical business processes;
- Identifying and considering the implementation of additional preventive and mitigating controls;
- Identifying sufficient financial, organisational, technical, and environmental resources to address the identified information availability requirements;
- Establishing and implementing a BC strategy, endorsed by management;

- Formulating and documenting Business Continuity Plans (BCPs) that address information availability requirements in line with the agreed BC strategy;
- Regular testing and updating of the plans and processes put in place;
- Ensuring that BC management is incorporated in Triangle processes and business-as-usual activities;
- Assigning responsibility for the BC management processes at appropriate management levels throughout Triangle.

See the Business Continuity Strategy and Disaster Recovery Plan for more information.

.

17 Policy Review Date

This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.