RIDGE

INFORMATION SECURITY DOMAIN POLICY

CONTENTS

1. DOCUMENT CONTROL 3

1.1. Distribution 3

1.2. Version Control 3

1.3. Applicable Documents 3

1.4. Definitions and Abbreviations 3

2. INTRODUCTION 4

2.1. Scope 4

2.2. Responsibilities 4

3. ASSET MANAGEMENT POLICY 4

3.1. Purpose 4

3.2. Principles 5

3.3. Information System Assets 5

3.4. Information Assets 5

3.5. Removable Media 5

4. ACCESS CONTROL POLICY 6

4.1. Purpose 6

4.2. Principles 6

4.3. Authentication 6

4.4. User Registration and De-Registration 7

4.5. Changes to Access Rights 7

4.6. Privileged Access 7

4.7. Review of User Access Rights 7

4.8. Password Management 7

5. MOBILE DEVICE AND REMOTE WORKING POLICY 8

5.1. Purpose 8

5.2. Principles 8

5.3. Mobile Device Configuration 8

5.4. Approved Devices 9

5.5. Network Access 9

5.6. Lost or Stolen Devices 9

6. CRYPTOGRAPHY POLICY 9

6.1. Purpose 9

6.2. Principles 9

6.3. Mobile Device Encryption 10

6.4. Database and Storage Encryption 10

6.5. Public Websites and Services 10

6.6. Transferring Data 10
6.7. Key Management 10
7. OPERATIONS SECURITY POLICY 11
7.1. Purpose 11
7.2. Principles 11
7.3. Documented Process and Operating Procedures 11
7.4. Change Management Policy 11
7.5. Capacity Management 12
7.6. Malware Protection Policy 12
7.7. Logging and Monitoring Policy 12
7.8. Vulnerability and Patch Management 13
8. BACK UP POLICY 14
8.1. Purpose 14
8.2. Principles 14
8.3. Performing Backups 14
8.4. Backup Restore 14
8.5. Backup Testing 14
8.6. Backup Monitoring 15
8.7. SaaS Backups 15
9. SUPPLIER SECURITY POLICY 15
9.1. Purpose 15
9.2. Principles 15
9.3. Procurement Engagements 15
9.4. Reassessment of Suppliers 16
9.5. Performance Monitoring 16
9.6. Contract Clause 16

1. DOCUMENT CONTROL

1.1. Distribution

This document, once issued, becomes a live document and, subject to updates and changes, shall be maintained as a configuration-controlled item. Any subsequent amendments must be submitted to the Systems Manager and controlled using document versioning.

DISTRIBUTION

1.2. Version Control

VERSION	DATE	DESCRIPTION	CREATED BY	REVIEWED BY
1.0	23.09.2021	Creation	LS	DW
1.1	24.01.2022	Review	LE	DW

1.3. Applicable Documents

DOCUMENT TITLE	DOCUMENT LOCATION

1.4. Definitions and Abbreviations

ACRONYM	DEFINITION

2. INTRODUCTION

It is Ridge and Partners LLP (Ridge) policy to safeguard its information and the information of which it is the custodiam of, from the loss of confidentiality, integrity and availability. This requires the appropriate selection, operation and maintenance of people, process, and technical security controls.

Information that is processed, stored, and transmitted is at risk from theft, corruption, misuse, and loss, if directed actions are not taken to ensure its security.

This suite of Information Security Policies sets the direction for securing Ridge's information, through consideration of key information security control areas, aligned to the Information Security Management System – ISO 27001.

Compliance with this policy will be monitored by Systems Manager on an ongoing basis. Non-compliance to the policy will be reported through Ridge's Risk Management Framework and Disciplinary process. This policy will be reviewed and updated, at yearly intervals, or where environment changes dictate.

2.1. Scope

This policy applies to Ridge's Information and Information Systems; and all colleagues and third parties with responsibilities for identifying, implementing, operating, monitoring, and maintaining information security controls.

All exclusions from scope are documented within the Statement of Applicability.

2.2. Responsibilities

- Equity Partners within Ridge have ultimate responsibility for ensuring compliance with this policy.
- Information Asset Owners have the responsibility of implementing this policy with regards to the assets they own.
- All staff shall adhere to this policy and handle information assets according to their classification.

3. ASSET MANAGEMENT POLICY

3.1. Purpose

This policy defines Ridge's approach to Information Security Asset Management, directly supporting the achievement of the following statement:

Information System assets shall be inventoried, accounted for, and understood, in terms of their criticality of supporting business operations. Assets shall have an assigned owner, who is responsible for the asset's 'lifecycle' planning and protection. Information Assets shall be classified and handled, according to their sensitivity. The classification determines how the information is to be 'handled'. Information Assets shall be retained according to Ridge's Data Retention Policy.

3.2. Principles

- Information System and Information Assets shall be inventoried, and their criticality understood.
- Asset registers shall be maintained, and the asset landscape reported on.
- Security shall be planned for throughout the assets lifecycle.

3.3. Information System Assets

- All assets that process, store, or transmit Ridge's information shall be inventoried, regardless of how the asset is delivered (e.g., As a Service or On-premises).
- System assets fall into three classes: Software, Infrastructure and Hardware. These assets shall be documented on appropriate, and routinely maintained asset registers.
- As a minimum, the asset registers shall record:

    a. The asset description,
    b. The assigned asset owner,
    c. The asset's location,
    d. The asset's criticality categorisation: Low, Medium, High (impact caused if the asset should become unavailable) and,
    e. Appropriate management information, including serial, version, and licensing numbers.

- Asset Owners shall appropriately plan for the asset's implementation, maintenance, return, decommissioning / reconditioning and secure disposal. Such plans shall carefully consider the requirements of Ridge's Information Security Policies. Where the asset is assigned to an end user e.g., laptop and mobile phone, responsibilities for asset planning shall reside with the users Line Manager.
- A formal management process for the secure sanitisation and disposal of information system assets shall be documented. This shall include appropriate secure 'wiping' and destruction techniques, use of any third-party disposal services and record keeping.
- Periodic reviews of the asset register shall be performed, to ensure its accuracy.

3.4. Information Assets

- Information Assets shall be categorised and handled in accordance with the Information Classification and Handling Policy.

3.5. Removable Media

- The use of removable media (including USB's, external hard drives, tapes, CD's etc.) is prohibited, unless explicitly approved, and issued by Ridge.
- Removable media shall only be used in cases where no suitable alternative exists (e.g., sanctioned network shares/cloud storage).
- Connecting removable media devices to Ridge's Information Systems is prohibited, unless explicitly approved by the [IT Department].
- Any use of removable media should be considered temporary and returned to the [IT department] soon as it is no longer required for its original task.
- Approval for policy exceptions can be obtained through the Systems Manager.

4. ACCESS CONTROL POLICY

4.1. Purpose

This policy defines Ridge's approach to access control, directly supporting the achievement of the following statement:

Access to Ridge's Information and Information Systems shall be appropriately controlled, determined by the operational needs of the business. Access shall be provisioned, according to the Users role, to an appropriate level that allows them to perform their duties, for as long as is necessary. Industry recognised authentication mechanisms shall be applied to the information being accessed. This may include multiple factors, subject to the sensitivity of the information being accessed. Users with elevated privileges e.g., administrator rights shall be subject to further controls.

4.2. Principles

- Access to Information and Information Systems shall be provisioned on a need-to-know and a least privileged basis.
- Active Directory (AD) shall be used as the primary mechanism for authenticating User accounts, including federating with Single Sign On (where possible).
- All AD User Accounts shall operate Multi-factor Authentication, and where possible, this should extend to all User Services that contain sensitive information.
- Duties of Users and Privileged Users shall remain segregated.
- The use of Generic User accounts shall be avoided.
- User and Service account passwords shall meet a defined level of complexity, and not be reused.

4.3. Authentication

- Ridge's AD system is the core authentication mechanism and should be used by any service requiring User account authentication, including federating to non-AD or cloud services with Single-Sign-On (where possible). All AD User and Service Accounts shall operate two-factor authentication, this should be extended to all accounts (where possible).
- AD Groups should be used to grant access to systems or aspects of systems, maintaining a list of who has access to which systems.
- Where systems cannot use AD credentials, they shall follow the same principles of need-to-know and least-privilege. Additionally, they shall follow an access control process ensuring that local ownership is applied by the Asset Owner. The process shall define steps taken to keep the access control list up to date.
- All User accounts, where possible, shall be set to automatically 'lock' following a failed number of logging attempts:

    a. User Accounts – 10 failed attempts.
    b. Elevated User Accounts – 2 failed attempts.
    c. Service Accounts – 2 failed attempts.

4.4. User Registration and De-Registration

- A 'New Starters' process shall be established to request, approve and provision User accounts and system access for new Users.
- A 'Leavers' process shall be established to promptly identify and revoke system access of User's departing the organisation. Accounts shall be disabled on the User's last working day.
- Inactive User accounts shall be set to automatically disable after 3 months. This shall prompt a review of the account.
- All processes shall be appropriately documented and be auditable.

4.5. Changes to Access Rights

- An 'Additional Access Request' process shall be established to request, approve and provision additional levels of access for existing Users. The additional access request shall be considered on a time-bound and permeant basis.
- A 'Movers' process shall be established to request, approve and provision system access, aligned to a new role within the organisation. The access shall be provisioned by disabling all existing access, before granting access required of the new role.
- All processes shall be appropriately documented and be auditable.

4.6. Privileged Access

- The provisioning of User accounts with elevated privileges, such as administrators, shall be controlled and restricted to those Users who have a defined and specific need to manage information systems or networks. These accounts shall remain segregated from a standard User account.
- Administrators shall be assigned an individual administrator account, used for system administrative purposes only.
- Administrator Accounts shall use Multi-factor Authentication and have access to email removed.
- Administrators shall be granted the least access possible to allow them to complete their duties. Full Domain Administrator accounts shall only be used when no other alternative is available.
- Service Accounts should be unique to each service.
- Default passwords/codes or equivalent shall be changed prior to use for all privileged accounts.
- Standard Users shall not be granted local administrator privileges, and therefore will be deliberately limited on what they can install/configure on their devices.

4.7. Review of User Access Rights

- Asset owners shall review the access levels for all Users on at least an annual basis.
- The IT Department shall review the AD access control list for anomalies, on at least a monthly basis.
- The Access Control reviews shall be documented and auditable.

4.8. Password Management

- Passwords shall include a mixture of upper- and lower-case characters, numbers and special characters such as :! , #, £, $.
- Password selection should feature a rememberable complex phrase, made up of 3 or 4 words e.g., WetPurpleCat!25.
- Passwords should never be shared or disclosed.

- Password Manager's, approved by Ridge are authorised for use. These shall have Multi-factor Authentication applied. Such requests shall be made via the IT Service Desk.
- Administrator, Service accounts and root passwords shall be set with strong passwords consisting of at least [12 characters].
- Passwords shall be changed at regular intervals. Where achievable, IT systems shall force password changes at specified intervals.
- Passwords should not be reused across services/systems, and where achievable, password history re-use policies shall be applied.
- Immediate action shall be taken by the User to change their system password, if for any reason, they suspect it has been compromised.

5. MOBILE DEVICE AND REMOTE WORKING POLICY

5.1. Purpose

This policy defines Ridge's approach to the use of mobile devices and secure remote working, directly supporting the achievement of the following statement:

The use of Mobile Devices (laptops, tablets and smart phones) and adoption of remote working practices supports greater operational flexibility, providing 'anytime anywhere' access to information and information systems. However, such availability must be balanced with appropriate security to prevent unauthorised access.

Only approved mobile devices are authorised to access Ridge's information and information systems. All devices shall be securely configured and have their security provisions maintained. Devices connecting to Ridge's IT Network, shall do so via dedicated secure access points.

5.2. Principles

- Mobile Devices shall be securely configured, aligned to current industry practice.
- Information and Information Systems shall only be accessible via Ridge 'approved' devices.
- The use and access of any personal devices is restricted to the Office 365 Application suite.
- Mobile Devices shall only access Ridge's IT internal Network via a dedicated VPN instance.
- Appropriate actions shall be taken to safeguard against the risks of lost and stolen devices.

5.3. Mobile Device Configuration

- Mobile Device platforms, where guidance and operational requirements permit, shall be configured according to industry recognised secure guidelines (e.g., NCSC Device Security Guidance).
- Mobile Devices shall have the following security features enabled by default:

    a. Remote disabling and erasure functionality,
    b. Malware protection (including automatic updates),
    c. Software installation restrictions,
    d. Automatic security (patches) updates,
    e. Disk encryption (where achievable),
    f. Complex password / Pin / Biometrics,
    g. Automatic 'screen locking' after 5 minutes of inactivity, and

h. Automatic 'device locking' after 10 failed logging attempts.

- Smart phones and tablets owned by Ridge, shall have Mobile Device Management (MDM) Software installed.

5.4. Approved Devices

- Only those Mobile Devices issued and or approved by Ridge's IT Department are authorised to access Ridge's information and information systems.
- Users of personal devices are responsible for arranging the devices configuration with the IT Department, prior to use. Only those Personal devices meeting the requirements of this policy shall be approved for use.
- An Asset register of all Ridge issued, and approved Mobiles Devices shall be maintained. The register shall be associated with the Starters / Movers / Leavers process.

5.5. Network Access

- Access to Ridge's IT internal Network shall be via a dedicated VPN instance. The VPN shall have Multi-Factor-Authentication enabled.
- Conditional access, where permitting, shall be used to authenticate Mobile Device connecting to Ridge's IT Network, including accessing third party hosted services.

5.6. Lost or Stolen Devices

- Mobile Device Users, upon accessing Ridge information (whether the device is issued by Ridge or personally owned), are responsible for reporting lost or stolen devices, immediately upon discovery, to the IT Department.
- Appropriate action shall be taken by the IT Department to remotely 'wipe' and disable access of reported lost and stolen devices.
- For stolen devices, the IT Department shall file a police report, obtaining a Crime Reference Number (CRN).

6. CRYPTOGRAPHY POLICY

6.1. Purpose

This policy defines Ridge's approach to cryptography, directly supporting the achievement of the following statement:

Cryptography plays a vital role in protecting the confidentiality and authenticity of information and information systems. Ridge shall effectively apply industry recognised cryptography controls to its most sensitive information, as it's been transmitted and stored, whilst taking appropriate steps to keep cryptography keys secret.

6.2. Principles

- Safeguard cryptographic keys against unauthorised disclosure, modification, loss and use.
- Apply cryptographic controls to Ridge's most sensitive information (Restricted) that is transmitted or stored.

- Only use encryption algorithms that are recognised by 'industry' as effective.

6.3. Mobile Device Encryption

- All Mobile Devices require encryption 'at rest' to protect Ridge's information. Devices operating Microsoft Windows 10 or later, shall enable BitLocker drive encryption.
- Devices running alternative operating systems shall either enable native encryption or enable drive encryption through installed Mobile Device Management Software.

6.4. Database and Storage Encryption

- Databases or network / cloud storage containing Ridge's most sensitive information (Restricted), shall be encrypted by default, unless an expectation has been agreed by the Systems Team Manager. As newer technology includes 'greater native encryption options, these should be enabled by default.
- Application Programming Interfaces (API's), associating Ridges internal systems, and where at least one of those systems contains sensitive information (Restricted), shall be secured with the TLS protocol version 1.2 or greater.

6.5. Public Websites and Services

- All Ridge public facing websites or systems containing data input fields and logons shall be secured with the TLS protocol version 1.2 or greater, and have a valid certificate issued by a recognised certificate authority.
- Any third-party service or hosted system shall be secured with TLS encryption version 1.2 or greater, as a minimum on any login, data entry or page displaying Personal, or Restricted business data.
- API's, associated with Ridge's public facing websites and systems shall be secured with the TLS protocol version 1.2 or greater.

6.6. Transferring Data

- Internet and cloud-based transit traffic shall always TLS encryption version 1.2 or greater enabled unless a valid exception has been approved.
- Email shall apply opportunistic TLS for all outgoing email.
- Use of removable media devices is restricted, however if approved for a specific purpose and used to transfer sensitive business information, the device shall be hardware encrypted using minimum AES 256 encryption, issued by Ridge.
- Enhanced tools beyond regular email include built-in encryption in Microsoft Office products and Microsoft SharePoint. The requirements of when these tools should be applied is defined in the Information Classification and Handling policy.

6.7. Key Management

- A procedure for the secure management of cryptographic keys, to control both the encryption and decryption of encrypted data or digital signatures shall be adopted. In line with industry practices, the procedure shall consider the keys: secure storage, expiry, access control and auditioning.

7. OPERATIONS SECURITY POLICY

7.1. Purpose

This policy defines Ridge's approach to operations security, ensuring correct and secure operations of information processing systems.

7.2. Principles

- Documented process and operating procedures, related to the effective operation of security controls shall be maintained, to the extent that they are deemed necessary.
- The impacts of information systems changes shall be understood and controlled.
- Available computer capacity resources shall never reach 100% utilisation.
- Information and Information Systems shall be protected against malware.
- A proactive capability to identify and respond to security events and alerts, that have the potential to impact service delivery, shall be maintained.
- A record of security events, generating digital forensics shall be securely retained for a specified period.
- The exploitation of technical security vulnerabilities shall be appropriately managed.

7.3. Documented Process and Operating Procedures

The operation and maintenance of security controls require secure and consistent application; removing the opportunities for induced vulnerabilities to occur. Ridge shall take the following steps to ensure secure and repeatable practices are applied to its security controls.

- Information Security policy requirements shall be planned for, considering the need for documented process and operating procedures. Such considerations should include:

    a. Complexity of the operation.
    b. The opportunity for a state of subjectivity to arise.
    c. Highly specialist operations.
    d. The opportunity for ineffective decision making to occur.

7.4. Change Management Policy

Uncontrolled changes to information systems can induce exploitable security vulnerabilities or cause unexpected service interruption. Ridge shall take the following steps to prevent uncontrolled changes from taking place:

- Information System changes shall be controlled by the Change Assessment Board (CAB), in accordance with a formal control process.
- The control process shall ensure that proposed changes are reviewed, authorised, tested (where necessary), implemented, and released in a controlled manner; and that the status of each proposed change is monitored.
- To satisfy the requirements of this policy, the following considerations shall be implemented:

    a. Proposed changes to information systems shall be assessed for service delivery and security risks, against a defined framework. This shall include determining the type of change e.g., routine, non-routine and emergency.

b. Appropriate and documented control plans shall be put in place to manage change risks to an acceptable level e.g., phased deployment, roll back plans etc.
c. Change risks that cannot be managed to an acceptable level shall be either rejected by the CAB or escalated to the IT Partner.
d. Changes shall be sufficiently documented.

7.5. Capacity Management

Capacity management is essential to ensuring critical services continue to run effectively. Ridge shall take the following steps to manage its computer capacity resources:

- The use of computer resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required systems performance.

7.6. Malware Protection Policy

Malicious software (Malware) is software or web content that can inflict serious harm to Information and Information Systems. Ridge shall take the following steps to protect against the threat of malware.

- All Ridge managed clients, mobile devices and servers shall have malware protection installed. The malware protection shall be centrally managed; constantly checking for updates and deploying updates at short notice
- All third-party servers, hosting Ridges information shall have malware protection installed.
- Ridge shall further enhance its malware protection through employing a defence in depth approach, utilising network tools. This shall include:

    a. Web traffic inspection
    b. Secure web gateway
    c. Secure email gateway

- Ridge's Information Systems shall be monitored for malware alerts or suspicious activity, 'triggering' an appropriate response.

7.7. Logging and Monitoring Policy

Security monitoring is an essential component in the identification and detection of cyber threats. It provides network and system, visibility when detecting and recovering from security incidents, whilst providing assurance that devices are being used in accordance with policy.

Effective monitoring relies on proportionate and reliable logging practices. This policy shall observe these practices, reflected in the following requirements:

- A separate logging and monitoring strategy shall identify the most valuable log sources available to Ridge; with the aim of maintaining an appropriate audit trail and presenting evidence in the wake of a security incident. The strategy shall further consider data retention and storage requirements, and the frequency in which monitoring shall be performed.
- The log sources, identified within the strategy, shall include consideration of system events, user activities, exceptions, faults, security events, system administrator and system operator activities
- Access to log information shall be provisioned on the principles of 'need-to-know' and 'least privileged'.
- System administrators shall be prohibited from erasing or de-activating logs of their own activities.

- The clocks of all Domain joined information systems within Ridge, shall be synchronised by Active Directory.

7.8. Vulnerability and Patch Management

Exploitation of known security vulnerabilities remains one of the greatest causes of security incidents. Timely applying software and firmware updates to vulnerable Information Systems is vital in preserving information security. The policy shall observe these practices, reflected in the following requirements.

- Vulnerability scans shall be performed regularly or on request using a dedicated solution running up-to-date plugins. The scans shall cover both externally and internally facing information services.
- External penetration tests shall be performed, supplementing, and validating the results of the internal capability. This shall be planned to take place at least annually, testing all externally facing services.
- Supplementary penetration tests shall be required prior to the commissioning of new Information Systems, or if significant changes have been made to an existing system.
- The results of vulnerability scans and penetration test shall be prioritised for remediation according to criticality. To aide in the prioritisation the Common Vulnerability Scoring System (CVSS) shall be utilised.
- Information Security shall oversee the remediation of vulnerabilities performed by IT, adhering to the timescales defined in table one.

Table One – Vulnerability Remediation

VULNERABILITY SEVERITY	CVSS SCORE	REMEDIATION TIMEFRAME
Critical	9.0 - 10.0	• Create corrective action plan within 7 days • Remediate vulnerability within 14 days
High	7.0 -8.9	• Create corrective action plan within 14 days • Remediate vulnerability within 28 days.
Medium	4.0 – 6.9	• Create corrective action plan within 28 days • Remediate vulnerability within 3 Months
Low	0.1 – 3.9	• Based on availability of resources

In addition, Microsoft Patch Tuesday releases, shall be applied within 8 calendar days.

- Where it is not feasible to remediate a vulnerability in the given timeframe, the impact of not doing so shall be further assessed as an information security risk.
- Where possible, Ridge shall aim to run the latest stable version of a given software and firmware, and only previous versions provided that it remains supported, in order to maintain stability.
- Where there is no other viable option but to tolerate unsupported systems, NCSC guidance for securing obsolete platforms shall be followed. In addition, the risk the unsupported system presents, shall be further assessed as an information security risk.
- All managed Windows clients shall receive Windows updates on a regular basis, distributed and monitored centrally.
- All servers shall be included in a rolling monthly patch schedule.

8. BACK UP POLICY

8.1. Purpose

This policy defines Ridge's approach to data backups, directly supporting the achievement of the following statement:

Performing regular backups of Ridge's most important data, is vital step in allowing business services to continue to function, following the impact of a natural disaster or security incident. Ridge shall effectively apply industry recognised back up practices, ensuring it has confidence that it can recover its most important data, when it is relied upon.

8.2. Principles

- The frequency and extent of backups is determined by the importance of the information.
- The backup media shall be stored with sufficient protection and in appropriate environmental conditions.
- Backups shall be tested to ensure that they are recoverable.

8.3. Performing Backups

- Ridge's information shall be backed up periodically. The frequency and extent of backups must be in accordance with the importance of the information, and as documented within a backup schedule.
- The backup schedule shall consider the Recovery Point Objective of the information, determining the most suitable type of back up strategy e.g., full, partial, incremental etc.
- The backup strategy shall be 'underpinned', as a minimum, by the industry recognised 3,2,1 backup rule (3 copies, on 2 separate devices and one offline). The offline backup shall be physically stored away from the production site.
- Backup media devices shall be secured with appropriate physically security controls e.g., access control.
- Where achievable, 'write once' configuration rules shall be applied to backups, preventing them from being overwritten.
- Data backups shall be encrypted using native encryption within backup software, as a minimum.
- The process for performing backups shall be documented, and only carried out by suitably trained colleagues.

8.4. Backup Restore

- The process for restoring from a backup shall be documented, and only carried out by suitably trained colleagues. ÁÁ
- An audit trail of the restoration process shall be maintained, and retained, for at least 12 months.
- Access to backups shall be provisioned on need-to-know and a least privileged basis, supported by Multi-Factor Authentication.

8.5. Backup Testing

- Backups must be periodically tested to ensure that they are recoverable. To confirm media reliability and information integrity, the back-up information shall be tested in accordance with a specified testing schedule.

8.6. Backup Monitoring

- Backup software shall be configured to send failure and warning notification.
- Cloud backups shall be manually checked daily for issues.

8.7. SaaS Backups

- SaaS backups shall be carried out by the service provider, as contractually agreed.

9. SUPPLIER SECURITY POLICY

9.1. Purpose

This policy defines Ridge's approach to ensuring its supply chain its appropriately secured, directly supporting the achievement of the following statement:

Ridge shall apply a risk-based approach to the procurement of products and services, ensuring the level of risk posed is commiserate to the security resilience of the supplier and to the products and services being offered.

9.2. Principles

- Procurement engagements shall be assessed against the potential impact of a Confidentiality, Integrity and Availability compromise, before being categorised into a risk profile.
- Risk profiles shall detail the security requirements the supplier is expected to meet, and a record kept of their achievement.
- Periodic assessment of the suppliers ongoing security resilience and performance shall be made.
- New and or upgraded Information Systems shall demonstrate adherence to the NCSC 'secure by design' principles and undergo independent penetration testing before being commissioned.

9.3. Procurement Engagements

- Prior to the procurement of any products and services (including contract renewals), the information security risk presented by the engagement shall be first understood. This requires the completion of a risk impact assessment, and the determination of a risk profile.
- The Impact assessment shall be completed by the procurement lead and reviewed and approved by the Systems Manager, prior to the commencement of contract negotiations with the supplier.
- The supplier is expected to meet the requirements of the determined risk profile, prior to the start of the engagement. Where a supplier does not meet such requirements, a binding commitment to demonstrate adherence within 6 months of the start of the engagement may be an appropriate course of action, subject to the risk presented.
- Where binding commitments have been agreed, the Systems Team Manager shall confirm that they are delivered upon within the defined timescales. Where the supplier fails to fulfil its commitments, the Systems Team Manager shall consult Ridge's Legal Partner.
- The product and services being offered by the supplier are expected to demonstrate the NCSC 'security by design' principles. This shall be a mandatory requirement for all medium to high-risk engagements.
- All medium to high-risk engagements shall first undergo independent pen testing, before being commissioned.

- The Systems Team Manager shall formally approve/reject the procurement engagement based on the available evidence presented by the supplier. Where Information Security reject an engagement, the procurement event should not progress any further until the risk has been further assessed and documented on the Information Security Risk Register.
- Information Security shall maintain an up to data inventory of all suppliers, along with the determined outcome, contract expiry date and Assessment date.

9.4. Reassessment of Suppliers

- Suppliers shall have their security resilience re-assessed on a periodic basis. It is reasonable to adopt a risk-based /risk-sampling approach to the assessments e.g., the most critical suppliers are reassessed annually, focusing only on any changes to the security posture that have occurred.
- and practical to make the assessment based on risk sampling e.g., changes to security resilience since the last assessment.
- Where suppliers no longer meet the expected security requirements, binding improvement plans shall be agreed, and delivered by the supplier within 6 months.
- Where a supplier has been previously assessed under a separate engagement, and a new engagement arises, the supplier shall be reassessed if the new engagement presents a 'higher' risk profile.

9.5. Performance Monitoring

- Appropriate arrangements shall be put in place to ensure the contract is being delivered as expected, and that any changes to the supplier's security resilience, including security incidents, is communicated to Ridge.

9.6. Contract Clause

- Appropriate information security clause shall be represented in the commercial contract, as a minimum, this shall include:

    a. Declaration of accuracy to the submitted security resilience evidence.
    b. The right to audit.
    c. Notification of serious security breaches and critical security vulnerabilities.
    d. Changes to security resilience.
    e. Compliance to the Data Protection Act 2018.
    f. Agreement of improvement plans (where identified).