



Security Management Plan

e: info@redactxpert.ai

w: <https://www.redactxpert.ai>

Powered by Simpson Associates



Contents

1. Introduction.....	3
1.1 Purpose	3
1.2 Scope	3
2. Security Governance.....	3
2.1 Organisational Structure	3
2.2 Security Objectives and Principles	3
2.3 Roles and Responsibilities	4
3. Policies and Standards.....	5
3.1 Standards & Certifications	5
3.2 Policies	5
3.3 UK Police-Assured Secure Facilities (PASF)	5
4. Risk Management.....	5
4.1 Risk Assessment Scope.....	5
4.2 Business Impact Assessment.....	5
4.3 Risk Assessment	7
4.4 Controls	11
5. Asset Management.....	14
6. Access Control and Identity Management	14
7. Data Security and Privacy	15
8. Application Security.....	15
8.1 Secure Development Practices	15
8.2 Code Review and Testing Practices.....	15
8.2.1 Code Review	15
8.2.2 Testing.....	16
8.3 Environments	16
8.3.1 Environment Separation.....	16
8.3.2 Data and Access Controls	16
8.3.3 Approvals	16
8.4 Software Supply Chain Security	17
8.4.1 Approved Package Repositories	17
8.4.2 Dependency Management	17
8.4.2.1 Vulnerability Scanning.....	17
8.4.2.2 Licence Management	17
8.4.3 OS/Software Patching.....	17
9. Logging, Monitoring, and Alerting.....	18
10. Incident Management	18
11. Business Continuity and Disaster Recovery.....	18
12. Third-Party and Supplier Security.....	18
12.1 Supplier Due Diligence and Onboarding	18
12.2 Third Party Supplier Register	19
13. Personnel Security	19
13.1 Vetting.....	19
13.2 Security Awareness and Training	19

1. Introduction

1.1 Purpose

This Security Management Plan (SMP) outlines the comprehensive security measures that are taken on RedactXpert to safeguard the confidentiality, integrity and availability of the RedactXpert platform and related data (including customer data). The SMP also covers how we manage security for personnel, information and assets and certifications across RedactXpert.

1.2 Scope

This SMP covers all environments of the RedactXpert SaaS platform (both production and non-production environments), as well as relevant, related areas of Simpson Associates (the providers of RedactXpert), such as personnel and assets.

Note that any activities conducted within Simpson Associates that are not directly related to RedactXpert are not covered by this plan.

2. Security Governance

2.1 Organisational Structure

RedactXpert is a product owned and managed by Simpson Associates Information Services Ltd (Simpson Associates). The parent company of Simpson Associates is Amari Group Ltd. RedactXpert itself is not an organization but is operated by a subset of employees within Simpson Associates.

Security governance processes for RedactXpert will therefore follow the same processes as for Simpson Associates, with additional considerations where needed for the RedactXpert platform itself.

2.2 Security Objectives and Principles

Security is a critical consideration for the RedactXpert platform. Given that information is being redacted, it is fully expected that sensitive data will be uploaded to the application, and therefore security is considered at all stages of the solution, from design, to implementation, to support and operations. More information on the security measures and controls put in place can be found in the Data Protection Policy.

2.3 Roles and Responsibilities

Effective security management for RedactXpert depends on clearly defined roles and responsibilities across, engineering, security, operations, and supporting business functions.

Although RedactXpert is delivered by a focused team within Simpson Associates, responsibilities span multiple disciplines to ensure the confidentiality, integrity, and availability of the platform. Roles are defined by capability and knowledge; this means team members may take on multiple roles, however Segregation of Duties is maintained by applying controls such as auditing, monitoring and management supervision.

Area of Responsibility	Primary Role(s)	Supporting Roles
Security Governance	Security & Compliance Lead	CISO
Security Policies & Standards	Security & Compliance Lead	Engineering Lead
Risk Assessment & Management	Security & Compliance Lead	Engineering Lead
Secure Architecture & Platform Security	Engineering Lead, Cloud Engineers	Security & Compliance Lead
Identity & Access Management (RBAC/PIM)	Engineering Lead, Cloud Engineers	Security & Compliance Lead
Secure Development & Code Review	Engineering Lead, Developers	Cloud Engineers
SAST & Dependency Scanning	Engineering Lead	Developers
Logging, Monitoring & Alerting	Cloud Engineers, Support Lead	Security & Compliance Lead
Incident Management & Customer Notification	Support Lead	Security & Compliance Lead
Data Protection & GDPR Compliance	DPO	Security & Compliance Lead
Data Retention & Deletion Controls	Security & Compliance Lead, Cloud Engineers	DPO, Support Lead
Business Continuity & Disaster Recovery	Cloud Engineers, Support Lead	Engineering Lead
Supplier Security Management	Engineering Lead	Security & Compliance Lead
Staff Vetting & Training	People Team	Security & Compliance Lead

3. Policies and Standards

3.1 Standards & Certifications

RedactXpert adheres to multiple standards and certifications as follows:

Standard/Certification	Date of Expiry	Scope of Accreditation
ISO 27001	20 th April 2027	Amari Group Ltd (Covering Simpson Associates and RedactXpert)
ISO 9001	20 th April 2027	Amari Group Ltd (Covering Simpson Associates and RedactXpert)
Cyber Essentials	22 nd August 2026	Simpson Associates (Covering RedactXpert)
Cyber Essentials Plus	24 th September 2026	Simpson Associates (Covering RedactXpert)

RedactXpert is committed to maintaining the highest levels of security and compliance with the relevant certifications as necessary. ISO 27001, ISO 9001, Cyber Essentials, and Cyber Essentials Plus are all renewed on a regular basis as part of Simpson Associates' ongoing operations.

3.2 Policies

All policies that apply to Simpson Associates employees, such as the Information Security Policy, Asset Management Policy, and Acceptable Use Policy, continue to apply to RedactXpert as well.

Additional policies and procedures are applicable specifically to RedactXpert and referenced throughout this Security Management Plan as follows:

- Business Continuity and Disaster Recovery Plan
- Change & Release Management Process
- Data Protection Policy
- Joiners Movers Leavers Process
- Support Access Process

3.3 UK Police-Assured Secure Facilities (PASF)

The RedactXpert solution also aligns with UK Police-Assured Secure Facilities (PASF) for hosting of the Azure services. Azure UK datacentres qualify for UK PASF as detailed [here](#). All RedactXpert Azure components are hosted within Azure UK regions and therefore meet this compliance initiative.

4. Risk Management

4.1 Risk Assessment Scope

The risk assessment is explicitly scoped to cover the RedactXpert SaaS platform itself and identify risks related to security of the platform, administrators, and data within the platform. The risk assessment does not cover Simpson Associates itself but builds upon the risk assessment and management approach as part of its ISO27001 accreditation.

4.2 Business Impact Assessment

Information uploaded to the RedactXpert platform is expected to be sensitive by the nature of it needing to be redacted and will in almost all cases contain personally identifiable information (PII). If this information

was to be leaked outside of the platform, then this could have severe implications in terms of damage to the individual(s) whose PII had been leaked, reputational damage to the business, and could also involve legal implications for the business.

4.3 Risk Assessment

Risk ID	Inherent Risk	Inherent Risk Level	Vulnerability	Controls	Residual Risk Level
R01	Internet attackers could hack the application.	Medium	The application is accessible on the public internet.	C01: Penetration testing C02: Azure cloud configuration review C03: Web application firewall C04: Private network restrictions	Low
R02	Users could maliciously or accidentally access documents within another tenant	High	Tenants utilise the same web portal and some shared services such as compute.	C01: Penetration testing C07: Application level RBAC C08: Tenant level data access controls C09: Tenant data storage isolation	Low
R03	Malicious code could be introduced as part of a deployment	Medium	Code is deployed to operate the service	C01: Penetration testing C06: Platform level RBAC C11: Just-in-time platform access C17: Environment segregation C19: Code review processes C20: SAST tooling C21: Automated dependency scanning	Low
R04	Attackers compromise management-plane resources, enabling alteration of platform	High	The platform relies on Azure control-plane services; compromised administrator identities could allow	C02: Azure cloud configuration review C04: Private network restrictions (no public access to internal resources).	Low

	configuration, deploy malicious resources, exfiltrate secrets, or weaken tenant-isolation and security controls.		elevation of privilege and widespread impact across environments.	C06: Platform level RBAC C11: Just-in-time platform access C12: Approval process for privileged platform roles C17: Environment segregation	
R05	A ransomware attack could encrypt or corrupt platform data, configuration assets, or operational systems, leading to loss of service availability and potential permanent loss of customer-uploaded data.	Medium	Ransomware can be introduced through compromised administrator identities, malicious code injection, supply-chain dependencies, or exploitation of platform-level misconfigurations. Although RedactXpert staff cannot access customer data, ransomware could still affect platform-level assets unless backups are strongly protected.	C02: Azure cloud configuration review C04: Private network restrictions C06: Platform-level RBAC (least privilege) C11: Just-in-time platform access C12: Approval process for privileged platform roles C17: Environment segregation C18: Use of password-less credentials C22: Secure credential management (Key Vault) C23: Immutable Backups	Low
R06	Denial-of-service Attack preventing legitimate users from accessing the service. This could cause prolonged service unavailability, disrupt	High	Attackers may attempt to overload network, compute, or application resources using volumetric, protocol-based, or application-layer DDoS attacks. Even though Azure	C03: Web-Application Firewall (WAF) C24: DDoS Protection	Low

	operational workflows for customers (including emergency services), and lead to reputational damage.		provides inherent baseline DDoS protections, targeted attacks could still degrade service availability unless resilience measures are implemented at multiple layers.		
R07	Incorrect configuration of Azure resources could expose internal services to the public internet, weaken tenant isolation, allow unauthorised access, or degrade security posture. Misconfigurations may occur through human error, incorrect deployment settings, or configuration drift across environments.	Medium	The RedactXpert platform relies on multiple Azure PaaS components. Although infrastructure is deployed and managed through controlled processes, misconfigurations remain a recognised risk in cloud environments. Such issues could allow unintended access to sensitive platform resources or weaken existing controls.	C02: Azure cloud configuration review C04: Private network restrictions C06: Platform-level RBAC C11: Just-in-time platform access C12: Approval for privileged platform roles C17: Environment segregation	Low
R08	Malicious or negligent insider misuse of application access leading to a data breach, fraud, or service disruption	High	Insider risk may arise from misuse of privileged access, abuse of administrative tooling, credential compromise, unauthorised configuration changes, or failure to follow secure operational procedures. Although production access is restricted and customer data is logically segregated,	C06: Platform-level RBAC C11: Just-in-time platform access C12: Approval for privileged platform roles C13: Staff Vetting C16: Access restrictions to customer data C25: SEIM Monitoring	Low

			individuals with elevated platform or support privileges could still impact confidentiality, integrity, or availability if access governance, monitoring, and segregation controls are not consistently enforced.	C26: Access Reviews C27: Joiners Movers Leavers Process	
--	--	--	---	--	--

4.4 Controls

Control ID	Control Title	Control Description	Further Information/Assurance Status
C01	Penetration testing	Annual penetration testing of the application is performed by a 3 rd party to identify security vulnerabilities.	Assured via external penetration test in January 2026 by a CHECK assured provider.
C02	Azure cloud configuration review	A review of Azure cloud configuration is performed annually to identify any security vulnerabilities or areas for increased security in the platform.	Assured via external cloud configuration review in January 2026 by a CHECK assured provider.
C03	Web-application firewall	WAF implemented to inspect and block malicious traffic, using OWASP 3.2 and Bot Protection.	Managed via Azure Application Gateway v2 WAF with OWASP CRS
C04	Private network restrictions	All resources in the solution (except access to the application itself) are protected by a private virtual network. Public access is disabled to resources and only communication internally between resources on the network is allowed.	
C05	TLS communication	All services communicate using TLS encryption in transit.	Minimum TLS 1.2
C06	Platform level RBAC	Access Permissions to all platform components are assigned via Role Based Access, ensuring security principals only have the minimum roles required (Users and system accounts). Admin permissions are tightly restricted and audited.	RBAC assignments reviewed as part of ISO27001 controls.
C07	Application level RBAC	Users within the RedactXpert application are assigned roles that define their access to features, ensuring least-privilege access to tenant data and operations.	
C08	Tenant level data access controls	Tenant boundaries within the application ensure users can only interact with resources belonging to their own organisation. Tenant context is validated on all operations.	Pen Test includes checks for lateral navigation within the application.
C09	Tenant data storage isolation	Tenant data is isolated in unique storage accounts and databases. Enterprise tenants are further isolated with individual database servers.	
C10	Tenant network isolation	Tenant data is isolated in per tenant virtual networks	
C11	Just-in-time platform access	Elevated privileges require JIT activation via PIM to minimise standing administrative permissions	All activations logged and reviewed via Azure PIM audit logs.
C12	Approval process for privileged platform roles	Requests for privileged roles must be approved by designated approvers before access is granted, ensuring strict segregation of duties.	Approvals evidenced within PIM logs

C13	Staff Vetting	All staff with access to the RedactXpert application and platform are vetted in line with the customer (and internal) vetting requirements.	For example, NPPV Level 3
C14	Sensitive column encryption	Database columns containing PII or other sensitive information are encrypted at the database level and protected with per-tenant RedactXpert managed key pairs.	Azure SQL Always Encrypted with Key Vault integration.
C15	Storage account file encryption	Storage containing uploaded documents uses encryption-at-rest enforced by Azure Storage Service Encryption.	
C16	Access restrictions to customer data	RedactXpert staff cannot access customer-uploaded data (documents or PII). Access is blocked by design, policy, and technical enforcement.	Enforced by encryption, RBAC, and application logic
C17	Environment segregation	Development, test, and production environments are kept separate via distinct subscriptions, credentials, networks, and deployment pipelines.	
C18	Use of password-less credentials	Interactions between platform components are performed with password-less managed service accounts.	Using Azure System Managed Identities with RBAC
C19	Code review processes	All code changes must be reviewed and approved via pull requests, preventing unauthorised code changes.	Azure DevOps Branch Security policies enforce all changes via PR
C20	SAST tooling	Static analysis security testing (SAST) is run during CI to detect insecure coding practices and vulnerabilities before code is deployed.	SAST scanning implemented in CI/CD pipelines.
C21	Automated dependency scanning	Dependencies are scanned for security vulnerabilities and licence issues automatically as part of CI/CD and via scheduled scans.	
C22	Secure credential management (use of key vault)	All secrets (keys, certificates, connection strings) are stored in Azure Key Vault and never committed to code or stored on developer machines. Access to secrets is tightly controlled and audited.	Use of secrets is kept to a minimum, with Managed Identity authentication used where supported.
C23	Immutable backups	Immutable, isolated backups protect against ransomware by ensuring data cannot be modified, encrypted, or deleted by attackers, even with elevated privileges.	Backups for audits, metrics, and global/central data are stored separately with write-once, read-many (WORM) retention. There are no immutable backups for tenant data as this is treated as ephemeral.
C24	DDoS Protection	DDoS protection is used to detect and mitigate malicious high-volume traffic to prevent service disruption and ensure system availability.	

C25	SIEM Monitoring	Centralised logging and real-time analysis of security events to detect, and respond to suspicious or unauthorised activity across systems and user accounts.	
C26	Access Reviews	Periodic verification of user permissions to ensure access remains appropriate to job roles and to promptly remove excessive or outdated privileges.	Access reviews are conducted every 6 months alongside being triggered by other events such as the Joiners Movers Leavers Process.
C27	Joiners Movers Leavers Process	Formal onboarding, role-change, and off-boarding procedures to provision access securely, adjust permissions as responsibilities change, and revoke access immediately when individuals leave the organisation.	

5. Asset Management

Only assets that are specific to RedactXpert are considered here. Assets that form part of Simpson Associates are not in scope of this security management plan.

Asset ID	Asset	Asset Type	Description
A01	Microsoft Entra Tenant	Platform	RedactXpert Entra tenant used for identity and access management.
A02	SaaS Production Application Platform (Azure)	Platform	RedactXpert Azure platform for the production environment.
A03	Cloudflare DNS	Platform	Cloudflare DNS hosting for RedactXpert domains
A04	RedactXpert Website	Platform	RedactXpert website (www.redactxpert.ai) hosted by Dock.
A05	Azure DevOps	Development	Azure DevOps organisation, project and repositories for storing RedactXpert application and platform code.
A06	Nutrient Portal & Licence Key	Development	Management portal for GdPicture.NET SDK licence key.
A07	Break Glass Account Yubi Keys	Physical	Yubi keys to support the break glass accounts login process.
A08	SQL Data Encryption Keys	Platform	Key pairs used to encrypt/decrypt sensitive data stored in SQL Databases.

6. Access Control and Identity Management

Microsoft Entra ID is used for identity management of RedactXpert operations teams. Individuals involved in RedactXpert are given explicit accounts within the RedactXpert tenant to use for accessing the RedactXpert platform. Accounts will not be shared. Per advice from the NCSC, password changes are not mandatory, and we will only change passwords when compromise is known or suspected.

Given that RedactXpert staff are a subset of Simpson Associates staff, these users will also have a Simpson Associates account which is maintained and managed in a separate Microsoft Entra tenant. This Simpson Associates account is used for things such as email correspondence, and access to code repositories to take advantage of licensing benefits within Simpson Associates.

More information can be found in the Joiners Movers Leavers Process.

The principle of least privilege is applied at all levels in the solution, including database access, access between resources in the solution, and platform administrator access. Segregation of duties is also performed via specific groups being used for certain functions/roles within the platform, with role-based access control (RBAC) being applied.

Privileged Identity Management (PIM) is used to provide advanced access control, with restricted access and approvals being required in privileged scenarios. All access via PIM is audited. More information can be found in the Support Access Process.

7. Data Security and Privacy

Data uploaded to the RedactXpert solution is, by its very nature, sensitive, and so security and privacy is factored into the platform by design. Best practices around security are followed in all areas such as encryption, private networking, data retention and deletion, data access, and data residency.

It is our policy that RedactXpert staff cannot access the data that is uploaded by customers, including the document contents and any sensitive metadata such as PII detected by the solution. This is enforced via policy and encryption levels.

More information can be found in the Data Protection Policy.

8. Application Security

8.1 Secure Development Practices

Security is considered at all stages of the development lifecycle and factored into both design and implementation. RedactXpert adheres to industry standards and best practices, including referencing OWASP resources such as the OWASP Top 10 vulnerabilities as part of development and code review.

8.2 Code Review and Testing Practices

8.2.1 Code Review

Code for the RedactXpert solution is maintained within source and version control using Git.

All code developed for RedactXpert must be reviewed by another team member before being merged into the main branch as part of a pull request. Direct commits to the main branch are not allowed.

The pull request process includes the following checks, which must all be true before being completed:

- Code must be reviewed and approved by another team member
- CI/CD pipelines must be successfully completed. These involve the following:
 - The code must be built successfully
 - Automated tests must be successfully passed
 - Formatting checks must be successfully passed
 - Security scanning (SAST) must be successfully passed, with vulnerabilities addressed or not applicable
 - Automated dependency scanning must be successfully passed, with no vulnerabilities in 3rd party libraries and no license compliance issues
- Any comments added to the PR must be resolved

8.2.2 Testing

Multiple levels of testing are performed as part of the ongoing development and maintenance of RedactXpert. The following tests are performed during the lifecycle of the solution:

- Developer Testing
- Unit & Integration Testing
- Security Testing (SAST)
- Dependency Scanning
- Secret Scanning
- Functional/User Acceptance Testing
- Load/Performance Testing
- AI Model Accuracy Testing
- Penetration Testing
- Cloud Configuration Testing
- Accessibility Testing

8.3 Environments

The RedactXpert platform consists of 3 environments:

- Development
- Test
- Production

8.3.1 Environment Separation

These environments are segregated from each other by separate Azure subscriptions, separate resources, and separate virtual networks. Separate sets of credentials are used between environments wherever possible, such as separate service principals for Azure DevOps deployments.

8.3.2 Data and Access Controls

The production environment has strict access controls in place as described in the Data Protection Policy, specifically that RedactXpert staff cannot access data that is uploaded by customers, such as file contents or detected PII. These same restrictions are not applied in the test and development environments to assist with debugging and troubleshooting activities. For this reason, customers are not given access to the test or development environments and no customer data is uploaded or stored in these environments.

8.3.3 Approvals

Deployments to the production environment must be approved by a member of the technical team for RedactXpert. Note that this will follow the Change & Release Management Process.

8.4 Software Supply Chain Security

RedactXpert utilises third-party open-source and commercial software components as part of its application architecture. All dependencies are sourced from approved repositories, subject to automated vulnerability scanning, and reviewed for licensing compliance.

8.4.1 Approved Package Repositories

Repository	Description
NuGet	.NET packages and libraries
Npm	JavaScript/TypeScript packages and libraries including Angular
Docker Hub	Microsoft ASP.net container base images
Google Chrome	Google Chrome installation for document conversion

8.4.2 Dependency Management

8.4.2.1 Vulnerability Scanning

Third party libraries and packages are scanned for vulnerabilities automatically as part of security tooling within GitHub Advanced Security for Azure DevOps.

These scans occur as part of pull requests and must succeed with no licence/vulnerability issues detected for the pull request to be able to be completed.

Automated vulnerability scanning is also conducted weekly to detect any new vulnerabilities that have been identified in existing third-party libraries.

If vulnerabilities are identified in packages, we aim to update these as soon as possible in the solution.

8.4.2.2 Licence Management

Licenses are reviewed as part of the dependency management process, and as part of code reviews in pull requests submitted by developers. If libraries (or versions of libraries) are introduced that do not have a supported licence for use in the solution, then these are removed and the change is rejected.

It is possible for open-source libraries in the solution with appropriate licenses to move to a paid/commercial model on newer versions. In these cases, we review how and where the library is used in the product to determine the best course of action from:

- Replacing the library with an alternative library that achieves a similar function (with a compliant license)
- Re-building the functionality internally without using a third-party library
- Engaging in a commercial license with the third-party library
- Removing the library and its associated functionality from the solution

The decision-making process factors in information such as the criticality of the library to the product, the effort involved in replacing the library or re-building the functionality internally, and the cost of a commercial engagement.

8.4.3 OS/Software Patching

The RedactXpert platform is made up of platform-as-a-service (PaaS) services within Azure and as such OS and software-level patching is handled by Microsoft on the Azure resources themselves.

9. Logging, Monitoring, and Alerting

We capture logs to use for security auditing and monitoring including:

- Application-level logging and telemetry
- Security audits within the application
- Security audits at a platform level (e.g. Entra Sign-In Logs, Azure Activity Logs, Privileged Identity Management Activation Logs)

These logs are captured via tools including Application Insights, Microsoft Defender for Cloud, Microsoft Sentinel, and the RedactXpert application itself.

We ensure that relevant alerting is in place to warn of suspicious activity, such as when access is granted to be able to read data that has been uploaded by a customer.

Logs are retained in line with retention policies depending on the type of data being collected. Details of the retention policies in place can be found in the Data Protection Policy.

10. Incident Management

Incident management will follow Simpson Associates' Incident Management Policy. In addition, upon awareness of a security breach/incident we will:

- Minimize the extent of actual or potential harm caused by the breach
- Remedy the breach to the extent possible
- Apply a tested mitigation against the breach
- Prevent a further security breach in the future that exploits the same root cause failure

Where necessary, we will notify relevant customers where a breach has (or has potentially) impacted them.

11. Business Continuity and Disaster Recovery

Customers rely on RedactXpert to greatly improve the speed, accuracy and security of their document redaction processes. If the service is unavailable, the only alternative available to most customers is to fallback to manually redacting documents. For some customers, this is a viable option, however other customers have moved over to RedactXpert from other tools which they may no longer have access to.

Ensuring that RedactXpert is available and has appropriate business continuity plans in place is therefore critical. These are documented as part of the Business Continuity and Disaster Recovery Plan.

12. Third-Party and Supplier Security

12.1 Supplier Due Diligence and Onboarding

When appointing subcontractors and suppliers, we have a process in place to evaluate the supplier to determine their security posture and identify potential risks. When assessing suppliers the following information is reviewed:

1. The information security certifications held by the provider and the scope of such certifications.
2. The location of data storage and data processing.

3. Whether there is a requirement for a Data Processing Agreement / Addendum to cover the transfer and processing of personal data under GDPR and the Data Protection Act 2018.
4. If applicable, whether the service provides single sign on integration with Entra ID.
5. If applicable, whether the service natively supports multi-factor authentication
6. Whether they conduct, at least annually, regular information security risk assessments.

Supplier access is granted in accordance with the principle of least privilege.

After a supplier has been on-boarded, we operate a supplier register for which we conduct scheduled reviews against the supplier with respect to Quality and Information Security.

12.2 Third Party Supplier Register

All suppliers engaged by Simpson Associates are recorded on the supplier log. There is an indication on the supplier log as to where suppliers are core to the operational service of the RedactXpert platform.

13. Personnel Security

13.1 Vetting

Some customers (such as UK police forces) require individuals to be vetted that may have access to the relevant parts of the RedactXpert service. Where RedactXpert staff will need access to support these customer's instances and infrastructure, they are vetted to Non-Police Personnel Vetting (NPPV) Level 3 and have Security Check (SC) clearance. These are provided and managed through Warwickshire Police with staff vetted as part of Simpson Associates.

Where personnel are vetted, this is managed in line with Simpson Associates' process for monitoring and maintaining vetting status. The status of individuals is monitored regularly, and renewals are performed in a timely manner where needed.

Any additional vetting needs for individual customers would need to be discussed as part of procurement of RedactXpert.

13.2 Security Awareness and Training

Staff will undertake regular training as part of their employment with Simpson Associates, at least once annually, covering the following topics:

- General Security & Data Handling
- Phishing