CyberSycure

Standard Service Definition Document

Document Version

Date	Version	Revised By	Approved By	Description of Change
09 / 01 / 2024	1.0	*************	*************	Initial Version

1. Purpose

This document outlines the comprehensive cybersecurity services offered to government agencies by CyberSycure Ltd. It provides a detailed overview of the services, key features, benefits, pricing, service management, and other essential information necessary for Customers to understand and procure our services.

2. Service Description

Our Comprehensive Cybersecurity Services provide government agencies with end-to-end solutions to address their cybersecurity needs. From consultancy and architecture design to security testing, supplier assurance, and secure-by-design implementation, our services ensure robust protection of government assets and compliance with regulatory standards.

3. Scope of Services Offered

3.1 Cyber Security Consultancy & Architecture

Tailored consultancy for developing and implementing robust cybersecurity strategies and architectures, including risk management, compliance, and secure network design.

Key Features:

- Customised cybersecurity strategy development.
- Detailed architecture design considering infrastructure, applications, and data security.
- Ongoing consultancy support for strategy implementation and management.

Benefits:

- Enhanced resilience against cyber threats and data breaches.
- Compliance assurance with government standards and regulations.
- Cost savings through efficient resource allocation and risk mitigation.

3.2 Supplier Security Assurance

Comprehensive assessments and ongoing monitoring to ensure supplier security compliance, including assessment methodologies, risk analysis, and continuous monitoring.

Key Features:

- Robust assessment methodologies covering technical, operational, and compliance aspects.
- Detailed risk analysis and mitigation recommendations for each supplier.
- Regular monitoring and reassessment to ensure ongoing compliance.

Benefits:

- Strengthened supplier security posture and reduced supply chain risks.
- Enhanced vendor relationships through collaborative security assessments.
- Identifies and addresses vulnerabilities in third-party products or services before they impact government operations.
- Improved visibility and transparency into supplier security practices.
- Continuous monitoring to assure sustained supplier security over time.

3.3 Security Testing

Thorough testing and assessment of systems to identify and remediate security vulnerabilities, including penetration testing, vulnerability assessments, and detailed reporting.

Key Features:

- Comprehensive penetration testing covering networks, applications, and infrastructure.
- Automated and manual vulnerability assessments to identify weaknesses.
- Thorough reporting with prioritised remediation recommendations.

Benefits:

- Proactively identify and mitigate security vulnerabilities, reducing the risk of breaches and data loss.
- Identification and remediation of critical security vulnerabilities.
- Enhanced security posture and reduced exposure to cyber threats.
- Compliance with regulatory requirements and industry standards.
- Clear remediation guidance facilitating efficient patching and strengthening of security defences.

3.4 Secure-by-Design Implementation

Integration of security principles and best practices into the design and development process of government systems and applications, including security requirements elicitation, secure coding training, and adherence to industry standards.

Key Features:

- Integration of security principles and frameworks into the design and development process.
- Security requirements elicitation and adoption of industry best practices.
- Risk-driven activities for building appropriate and proportionate cybersecurity controls within digital services.
- Track adoption of cybersecurity principles throughout the lifecycle.

Benefits:

- Consultants with practical SbD tool implementation in various sectors (Automotive, Government, Energy).
- Developed SbD tool that has been endorsed by Cabinet Office to be deployed across UK government.
- Reduced risk exposure and minimised likelihood of cyberattacks and breaches.
- Cost savings by addressing security concerns early and avoiding costs.
- Enhanced compliance with industry standards (NIST, CAF) and regulatory requirements.
- Improved security culture and efficiency in resource allocation.
- Increased trust, and confidence with streamlined processes and continuous improvement.

3.5 ISO27001 & ISO27701 Gap Assessment & Implementation

Assessment and implementation of information security and privacy management systems, including gap assessments, policy development, and staff training for compliance with international standards.

Key Features:

- Thorough assessment of current information security and privacy management systems.
- Development and implementation of policies, procedures, and controls to address gaps.
- Training and awareness programmes for staff to ensure understanding and compliance.

Benefits:

- Alignment with internationally recognised cybersecurity and privacy standards.
- Enhanced data protection and privacy management practices.
- Improved organisational resilience and readiness for regulatory audits.

4. Service Management

Our service management processes ensure efficient handling of incidents, changes, service requests, problems, and service levels. We maintain open communication channels with customers, providing regular updates and fostering positive relationships.

4.1 Incident Management

We promptly address any service disruptions or security incidents reported by customers via email. Our team acknowledges the issue, assigns it a priority level, and works to resolve it within agreed-upon timeframes.

Responsibilities:

- Acknowledge and prioritise reported incidents.
- Escalate critical incidents for immediate resolution.
- Provide regular updates on incident status via email.

4.2 Change Management

Where applicable, we carefully manage changes to customer environments to ensure stability and security. All changes undergo assessment, testing, and approval before deployment, communicated to customers via email.

Responsibilities:

- Document and assess proposed changes.
- Conduct testing and obtain approvals.
- Communicate change activities to customers via email.

4.3 Service Request Management

We handle service requests efficiently via email, including configuration changes, access requests, and support requirements, ensuring timely fulfilment.

Responsibilities:

- Receive and log service requests via email.
- Prioritise and assign requests for resolution.
- Communicate progress and updates to customers via email.

4.4 Problem Management

We proactively address underlying issues impacting service quality by identifying root causes and implementing permanent solutions, communicated to customers via email.

Responsibilities:

- Investigate and analyse recurring incidents.
- Implement corrective actions and preventive measures.
- Provide regular updates on problem resolution via email.

4.5 Service Level Management

We monitor service performance against agreed-upon SLAs and KPIs, conducting regular reviews and recommending improvements, communicated to customers via email.

Responsibilities:

- Monitor service performance and identify improvement opportunities.
- Conduct regular service reviews with customers.
- Ensure compliance with contractual obligations.

4.6 Customer Communication and Relationship Management

We maintain open channels of communication with customers via email, providing regular updates, addressing inquiries, and fostering positive relationships.

Responsibilities:

- Establish clear communication channels via email.
- Proactively communicate service-related updates and incidents.
- Solicit feedback and act as trusted advisors via email.

5. Service Constraints

Whilst most of our services are consultancy-based and do not include specific products, we understand that operating in a flexible manner for our clients may sometimes introduce situations where such a requirement may arise. Where this is applicable our service constraints encompass maintenance windows, level of customisation permitted, and feature deprecation schedules. We schedule regular maintenance windows to ensure service reliability and performance, evaluate customisation requests on a case-by-case basis, and provide advance notice of any planned feature deprecation to minimise disruption and ensure service continuity.

5.1 Maintenance Windows

We schedule regular maintenance to ensure service reliability, security, and performance. Updates, patches, and enhancements are applied during off-peak hours to minimise disruption. Advance notice with impact and duration details is provided to customers.

5.2 Level of Customisation Permitted

We aim to accommodate customers' unique requirements but may have limits on customisation. Requests are evaluated based on compatibility, security, and service impact. We collaborate with customers to explore feasible options aligned with best practices.

5.3 Feature Deprecation Schedule

We periodically assess and update service features to meet industry standards and customer needs. Some features may be deprecated to streamline services or address security. Customers are notified in advance, with guidance on alternative solutions to ensure continuity.

6. Service Levels

CyberSycure prioritises all requests based on scope and level of service loss to ensure swift and effective resolution of customer faults. Incidents with substantial impact, or issues hindering a section of a business from fully functioning, are given higher priority.

The following priorities apply to incidents and service requests that cannot be immediately resolved.

Level	Description All times are working hours/days (Mon - Fri 09.00 - 17.30)	Target Fix Time*
P1	**Critical** Issues causing total loss of service or critical service failure, impacting all users and resulting in major disruption to business operations. (e.g., complete system outage, severe breach)	8 hours
Update frequency P1 & P2		**1 hr**
P2	**High** Issues causing partial loss of service to critical systems, impacting some users or affecting business-critical functionality. (e.g., degraded system performance, security incident affecting critical data)	16 hours
P3	**Medium** Issues causing partial loss of service, intermittently affecting some users or non-business critical systems. (e.g., intermittent connectivity issues, moderate system performance degradation)	24 hours
Update frequency P3 & P4		**8-16 hrs**
P4	**Low** Service requests for configuration changes or non-service-affecting issues, requiring minor adjustments or enhancements. (e.g., routine system updates, configuration modifications)	32 hours

*** Target Fix Time indicates the maximum time allowed for issue resolution from the time of reporting.**

*** Update Frequency indicates how often customers can expect updates on the status of their reported issue.**

Note: Customers can obtain the status of any call by contacting the Support team and providing the relevant ticket number. However, periodic updates will be provided on all raised tickets. CyberSycure will collaborate with the customer to agree on the priority level to prevent any confusion or mismatched expectations. In instances where incidents may require more time to resolve than anticipated, CyberSycure is committed to keeping customers informed of the incident status.

7. Data Extraction & Removal

Our data extraction and removal process is designed to ensure a seamless transition for customers, with clear guidelines and procedures in place. Upon termination of the service subscription, we commit to providing a simple and quick exit process. This includes returning all consumer-generated data, including content, metadata, structure, and configuration, in agreed-upon formats and standards. We understand the importance of data portability, and therefore, offer mechanisms to export/import data to other common services/technologies. Additionally, we provide a transparent pricing structure for data extraction or migration to another service provider, ensuring no hidden costs for our clients. As part of our commitment to data security and privacy, we guarantee the purge and/or destruction of consumer data from any retained computers, storage devices, and media in accordance with security accreditation standards.

8. Escalations & Complaints

If you sense that an issue isn't being dealt with promptly or isn't receiving the necessary attention or priority, please make use of the escalation routes provided below. When reaching out, ensure to include the relevant issue number, a brief overview of the problem, and why you believe escalation is warranted:

Escalation Level	Contact
Level 1	support@cybersycure.co.uk
Level 2	escalations@cybersycure.co.uk

Unfortunately, there are occasions where something goes wrong but we will always endeavour to resolve these issues through our Support Departments in a timely-manner.

If you would like to raise a complaint regarding the provided service: Initially, we advise requesting to converse with the individual(s) identified in this escalation document. Should you find that your concern or issue remains unresolved to your contentment, please direct your communication to our Support team via email: support@cybrsycure.co.uk.

Please be assured we will do all we can to offer a swift resolution.

9. Exclusions

As our services primarily focus on consultancy and advisory roles rather than product or hosting services, we do not provide hosting or infrastructure/development services. Therefore, Backup/Restore & Disaster Recovery functionalities are not within our service scope. Our expertise lies in advising and implementing cybersecurity strategies, policies, and controls to enhance organisational resilience and mitigate cyber threats.