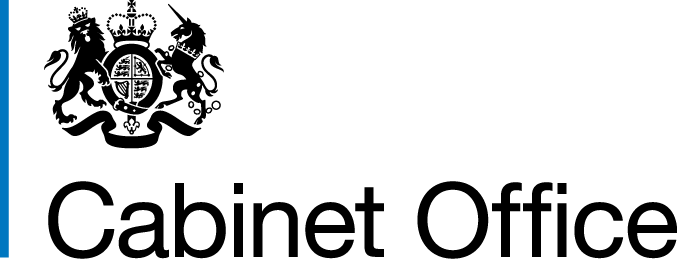
|  |
| --- |
| Commercial Information Assurance Team  Security Management Plan Template  Technical Delivery Partner and [Supplier Name]  Dated 2022 |

|  |
| --- |
|  |

****

Contents

[1 Executive summary 1](#_Toc102550409)

[2 System description 1](#_Toc102550410)

[3 Risk assessment 2](#_Toc102550411)

[4 In-service controls 4](#_Toc102550412)

[5 Supply chain security and third party subcontractors/tools 5](#_Toc102550413)

[6 Security requirements on participating departments, customers and users 5](#_Toc102550414)

[7 Personnel security 5](#_Toc102550415)

[8 Business continuity 5](#_Toc102550416)

[9 Physical security 5](#_Toc102550417)

[10 Major hardware and software and end of support dates 6](#_Toc102550418)

[11 Incident management process 6](#_Toc102550419)

[12 Required changes register 6](#_Toc102550420)

APPENDICES

[Appendix 1 ISO27001 and/or cyber essential plus certificates](#_Toc102550421)

[Appendix 2 Cloud security principles assessment](#_Toc102550422)

[Appendix 3 Protecting bulk data assessment if required by the authority/customer](#_Toc102550423)

[Appendix 4 Latest ITHC report and vulnerability correction plan](#_Toc102550424)

[Appendix 5 Statement of applicability](#_Toc102550425)

# Executive summary

1. [*This section should contain a brief summary of the business context of the system, the assurance work done, any off-shoring considerations and any significant residual risks that need acceptance.*]

## **Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date of Change** | **Change made by** | **Nature and reason for change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **References, links and dependencies**

| **ID** | **Document Title** | **Reference** | **Date** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## **Supplier personnel**

| **Key Personnel Names** | **Title** | **Contact Details incl. Mobile Number and Email Address** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |

# System description

## **Background**

* 1. [*A short description of the project/product/system. Describe its purpose, functionality, aim and scope.*]

## **Organisational Ownership/Structure**

* 1. [*Who owns the system and operates the system and the organisational governance structure. This should include how any ongoing security management is integrated into the project governance eg how a Security Working Group reports to the project board.*]

## **Information assets and flows**

### Logical data flow diagram

[*This should include a simple high level logical diagram on one page. The diagram must include any third party suppliers and the data flows to/from them.* ]

### Data assets

[*Include a table of the type and volumes of data that will be processed, managed and stored within the supplier system. If personal data, please include the fields used such as name, address, department DOB, NI number etc. Data processed by third party suppliers must be included here*]

## **System architecture**

* 1. *[A description of the physical system architecture, to include the system management. Please provide a diagram.]*

## **Users**

* 1. [*Please provide a table of the system users, this should include all users including HMG users as well as any service provider users and system managers. If relevant, security clearance level requirements should be included.*]

## **Locations**

* 1. [Please provide a table of where the Authorities data assets are stored, processed and any locations they are managed from. This must include the locations of any help desks or call centres if relevant. All third party suppliers and subcontractors must be included in this section. Any off-shoring considerations should be detailed with the legal basis for the data transfer included e.g. Standard Contractual Clauses, equivalency etc.]

## **Certifications**

* 1. [*Please include a table of any independent security certifications (eg ISO 27001:2013, Cyber Essentials Plus and Cyber Essentials) held as required by the contract. The table should include any relevant third party suppliers or subcontractors and must include the expiry date of the certification. Copies of the certificates should be included in Appendix 1.*]

## **Test and development systems**

* 1. [*Include information about any test, development and User Acceptance testing systems, their locations and whether they contain live system data.*]

# Risk assessment

## Accreditation/assurance scope

* 1. [*This section should describe the scope of the Risk Assessment and should indicate the components of the architecture upon which reliance is placed but assurance will not be done eg a cloud hosting service or a SAAS product/tool. A logical diagram should be used along with a brief description of the components. This scope must be agreed by the Authority.*]

## **Risk appetite**

* 1. [*A risk appetite should be provided by the Authority and included here.*]

## **Business impact assessment**

* 1. [*A description of the information assets and the impact of their loss or corruption (e.g. large amounts of Official Sensitive personal data the loss of which would be severely damaging to individuals, embarrassing to HMG, and make HMG liable to ICO investigations) in business terms should be included. This section should cover the impact on loss of confidentiality, integrity and availability of the assets and should be agreed with the Authority. The format of this assessment may be dependent on the risk assessment method chosen.*]

## **Risk assessment**

* 1. [*The content of this section will depend on the risk assessment methodology chosen, but should contain the output of the formal information risk assessment in a prioritised list using business language. Experts on the system and business process should have been involved in the risk assessment to ensure the formal risk methodology used has not missed out any risks. The example table below should be used as the format to identify the risks and document the controls used to mitigate those risks.*]

| **Risk ID** | **Inherent risk** | **Inherent risk level** | **Vulnerability** | **Controls** | **Residual risk level** |
| --- | --- | --- | --- | --- | --- |
| R1 | Internet attackers could hack the system. | Medium | The service systems are exposed to the internet via the web portal. | C1: Internet-facing firewalls  C2: Internet-facing IP whitelist  C3: System hardening  C4: Protective monitoring  C5: Application access control  C16: Anti-virus for incoming files  C54: Files deleted when processed  C59: Removal of departmental identifier | Very low |
| R2 | Remote attackers could intercept or disrupt information crossing the internet. | Medium | File sharing with organisations across the internet. | C9: TLS communications  C10: PGP file-sharing | Very low |
| R3 | Internal users could maliciously or accidentally alter bank details. | Medium-High | Users bank details can be altered as part of the normal business function. | C12. System administrators hold SC clearance.  C13. All changes to user information are logged and audited.  C14. Letters are automatically sent to users home addresses when bank details are altered.  C15. Staff awareness training | Low |

## **Controls**

* 1. [*The controls listed above to mitigate the risks identified should be detailed. There should be a description of each control, further information and configuration details where relevant, and an assessment of the implementation status of, and assurance in, the control. A sample layout is included below.*]

| **ID** | **Control title** | **Control description** | **Further information and assurance status** |
| --- | --- | --- | --- |
| C1 | Internet-facing firewalls | Internet-facing firewalls are in place between the internet and the system’, which restrict access from the internet to the required ports only. | Assured via ITHC firewall rule check |
| C2 | Internet-facing IP whitelist | An IP whitelist is in place for all access from the internet. | Assured via ITHC |
| C15 | Staff awareness training | All staff must undertake annual security awareness training and this process is audited and monitored by line managers. | Assured as part of ISO27001 certification |

## **Residual risks and actions**

* 1. [*A summary of the residual risks which are likely to be above the risk appetite stated after all controls have been applied and verified should be listed with actions and timescales included.*]

# In-service controls

1. [*This section should describe how the main security requirements as specified in the contract (security schedule) are met.*]

## **Protective monitoring**

* 1. [*This section should describe how your protective monitoring arrangements identify anomalous behaviour and how this is then acted upon as well as how logging and auditing of user activity is done.*]

## **Malware prevention**

* 1. [*This should describe how your anti-virus solution is implemented with respect to protecting Authority assets.*]

## **End user devices**

* 1. [*This section should detail the security controls which are implemented on all fixed and removable end user devices used to process, store or manage Authority data.*]

## **Encryption**

* 1. [*This section should detail the encryption measures you employ to protect Authority data both in transit and at rest.*]

## **Vulnerability management**

1. [*This section should detail your process for identifying, classifying, prioritising, remediating, and mitigating" software vulnerabilities within your IT environment.*]

## **Identity, verification and access controls**

* 1. [*This section should detail your password policy, your approach to ensuring that privileged accounts are accessible only from end-user devices dedicated to that use and by authenticated named users. This should include your use of multi-factor authentication for all accounts that have access to Authority data as well as privileged accounts.*]

## **Data Deletion**

* 1. [*This section should include the agreed process for securely deleting Authority data when required.*]

# Supply chain security and third party subcontractors/tools

1. [*This section should detail the assurance process for managing any security risks from Subcontractors and Third Parties authorised by the Authority with access to Authority data.*]

# Security requirements on participating departments, customers and users

1. [*Please detail any security requirements or codes of connection required by participating departments/agencies/third parties.*]

# Personnel security

1. [*Please provide details of your Personnel Security Vetting Policy for those staff who will have access to, or come into contact with Buyer data or assets.*
2. *Please provide details of how you will ensure that all staff accessing Buyer data are aware of the confidential nature of the data and comply with their legal and specific obligations under the Contract?*]

# Business continuity

1. [*Please provide an overview of your organisation’s business continuity and disaster recovery plans in terms of the Buyer data under the Contract, or attach a copy of your Business Continuity Plan.*]

# Physical security

1. [*Please provide details of the building where the service will operate from and describe the procedures and security in place to control access to premises and any areas holding Buyer assets. Detail measures such as construction of buildings used for handling Buyer assets, availability of lockable storage, procedures covering end of day/silent hours, key management, visitor controls.*
2. *Please also include details of any automated access controls, alarms and CCTV coverage. Please also provide details of the maintenance schedule of these security controls.> For the locations where Authority assets are held please provide details of any procedures and security in place designed to control access to the site perimeter. Please detail the measures in place such as fencing, CCTV, guarding, and procedures and controls to handle staff and visitors requesting access to the site. Please also provide details of the maintenance schedule of your security controls.*]

# Major hardware and software and end of support dates

1. [*This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.*]

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Version** | **End of mainstream Support/Extended Support** | **Notes/RAG Status** |
| Server Host | HP XXXX | Feb 2020/March 2022 |  |

# Incident management process

1. [*The suppliers’ process, as agreed with the Authority/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Authority/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.*]

# Required changes register

1. [*The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.*]

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ref** | **Section** | **Change** | **Agreed With** | **Date agreed** | **Documentation update** | **Status** |
| 1 | 6.4 | A new Third Party supplier XXXX will be performing the print capability. | Authority name | 11/11/2021 | Jul-2022 | Open |

1. ISO27001 and/or cyber essential plus certificates

[*Please include copies of the certificates here*]

1. Cloud security principles assessment

[*Please add your controls in the attached table.*]

| **Principle** | **Goals of the Principle** | **Controls** |
| --- | --- | --- |
| **Principle 1 – Data in transit protection**  "User data transiting networks should be adequately protected against tampering and eavesdropping." | • Data in transit is protected between end user device(s) and the service  • Data in transit is protected internally within the service  • Data in transit is protected between the service and other services (eg where APIs are exposed) |  |
| **Principle 2 – Asset protection and resilience**  "User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure." | Cloud service consumers should seek to understand:  • In which countries their data will be stored, processed and managed. They should also consider how this affects compliance with relevant legislation e.g. Data Protection Act (DPA), GDPR etc.  • Whether the legal jurisdiction(s) within which the service provider operates are acceptable to them |  |
| **Principle 3 – Separation between users**  "A malicious or compromised user of the service should not be able to affect the service or data of another." | Cloud service consumers should seek to:  • Understand the types of user they share the service or platform with  • Have confidence that the service provides sufficient separation of their data and service from other users of the service  • Have confidence that management of their service is kept separate from other users (covered separately as part of Principle 9) |  |
| **Principle 4 – Governance framework**  "The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined." | Cloud service consumers should ensure that:  • A clearly identified, and named, board representative (or a person with the direct delegated authority) is responsible for the security of the cloud service. This is typically someone with the title ‘Chief Security Officer’, ‘Chief Information Officer’ or ‘Chief Technical Officer’  • A documented framework exists for security governance, with policies governing key aspects of information security relevant to the service  • Security and information security are part of the service provider’s financial and operational risk reporting mechanisms, ensuring that the board would be kept informed of security and information risk  • Processes to identify and ensure compliance with applicable legal and regulatory requirements have been established |  |
| **Principle 5 – Operational security**  "The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes." | Cloud service consumers should be confident that:  • The status, location and configuration of service components (both hardware and software) are tracked throughout their lifetime  • Changes to the service are assessed for potential security impact. Then managed and tracked through to completion |  |
| **Principle 6 – Personnel security**  "Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel." | Cloud service consumers should be confident that:  • The level of security screening conducted on service provider staff with access to the consumers information, or with ability to affect the service, is appropriate  • The minimum number of people necessary have access to the consumers information or could affect the service |  |
| **Principle 7 – Secure development**  "Services should be designed and developed to identify and mitigate threats to their security.  Those which aren’t may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity." | Cloud service consumers should be confident that:  • New and evolving threats are reviewed, and the service improved in line with them  • Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment  • Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment |  |
| **Principle 8 – Supply chain security**  "The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement." | Cloud service consumers should seek to understand and accept:  • How their information is shared with, or accessible to, third party suppliers and their supply chains  • How the service provider’s procurement processes place security requirements on third party suppliers  • How the service provider manages security risks from third party suppliers  • How the service provider manages the conformance of their suppliers with security requirements  • How the service provider verifies that hardware and software used in the service is genuine and has not been tampered with |  |
| **Principle 9 – Secure user management**  "Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data." | Cloud service consumers should:  • Be aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone, web portal, email etc.)  • Ensure that only authorised individuals from their organisation can use those mechanisms to affect their use of the service (Principle 10 can help consumers consider the strength of user identification and authentication in each of these mechanisms) |  |
| **Principle 10 – Identity and authentication**  "All access to service interfaces should be constrained to authenticated and authorised individuals." | Cloud service consumers hould:  • Have confidence that identity and authentication controls ensure users are authorised to access specific interfaces |  |
| **Principle 11 – External interface protection**  "All external or less trusted interfaces of the service should be identified and appropriately defended." | Cloud service consumers should:  • Understand what physical and logical interfaces their information is available from, and how access to their data is controlled  • Have sufficient confidence that the service identifies and authenticates users to an appropriate level over those interfaces (see Principle 10) |  |
| **Principle 12 – Secure service administration**  "Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data." | Cloud service consumers should:  • Understand which service administration model is being used by the service provider to manage the service  • Be content with any risks the service administration model in use brings to the consumers data or use of the service |  |
| **Principle 13 – Audit information for users**  "You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales." | Cloud service consumers should:  • Be aware of the audit information that will be provided, how and when it will be made available, the format of the data, and the retention period associated with it  • Be confident that the audit information available will meet their needs for investigating misuse or incidents |  |
| **Principle 14 – Secure use of the service**  "The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected." | Cloud service consumers should:  • Understand any service configuration options available to them and the security implications of their choices  • Understand the security requirements of their use of the service  • Educate their staff using and managing the service in how to do so safely and securely |  |

1. Protecting bulk data assessment if required by the authority/customer

[*A spreadsheet may be attached*]

1. Latest ITHC report and vulnerability correction plan
2. Statement of applicability

[*This should be a completed ISO 27001:2013 Statement of Applicability for the Information Management System if ISO27001 certification is required by the contract.*]