GREATER**LONDON**AUTHORITY

Cyber Security Policy & Response Plan

Issue Date	January 2022 (Issue 1)
Amendments from previous version	Fundamental rewrite
Approved by	Executive Director of Resources
Review Date	December 2023
Senior owner	Executive Director of Resources
Document owner	Head of Information Technology

Contents

Cyber Security Policy

1. Purpose

1.1 This security policy sets out security requirements, roles, and responsibilities necessary to protect Greater London Authority (GLA) data and information systems from unauthorised access, inappropriate disclosure, or compromise. GLA senior management reviewed and approved this policy that is disseminated to staff, Members, and relevant external parties. The Head of IT (David Munn), Senior Systems Engineer Cybersecurity (Johnnel Olabhie), Cloud and Operations Manager (Stephen Askins), Programme Manager (Duminda Baddevithana) and Human Resources provided input and reviewed this document to ensure governing laws, regulations and GLA policies are appropriately incorporated. Furthermore, this security policy is defined in the context of the ownership of the GLA, legal and regulatory requirements, and takes into account industry security best practices.

1.2 Information and associated supporting processes, systems and networks are critical assets, the security of which is essential to serve Londoners and to maintain reputation, operational effectiveness, financial accuracy and legal compliance. The GLA is subject to a wide variety of increasingly sophisticated security threats, including viruses, hackers, computer-assisted fraud, espionage, sabotage, crime and natural disasters such as fire or flood. Increasing dependence on data, computer systems and services means the GLA is increasingly vulnerable to these threats. The requirement to interconnect our network with other GLA group members, stakeholders and partners makes cyber security increasingly complex.

1.3 The objective of cyber security is therefore to achieve and maintain a condition where all information, systems and networks are always available to those who are authorised to use them. Furthermore, that the data and information held by the GLA cannot be corrupted, is not disclosed to unauthorised persons, and its origin is authenticated. At the same time, it is important that cyber security is appropriate, proportionate, and integrated so that it will enhance, not impede, the work of the GLA.

1.4 The cyber security policy achieves this by defining rules and best practice in a range of areas:

- Identifying governance, information, systems and users
- Protecting information and systems through technical and cultural measures including staff training and awareness raising
- Detecting cyber-attacks through continuous monitoring
- Responding to cyber security incidents through well-defined response, management and communication plans
- Recovering information and systems following a security incident using well-practiced procedures

1.5 The cyber security policy applies to all GLA staff irrespective of status, including temporary staff, contractors, consultants, and third parties who have access to GLA data and systems. Cyber security is not purely a technical issue. All staff have an important responsibility to protect GLA

resources by being vigilant of cyber security risks at all times. This is achieved by staff taking responsibility for maintaining up to date knowledge of the cyber security policy, including rules and best practice governing online safety.

1.6 The purpose of this document is to specify and communicate the Greater London Authority cyber security policy.

2. Vision

The GLA aims to protect all its critical assets from Cyber threats. It uses a comprehensive, best-practice informed Cyber Security framework to ensure that services are not disrupted, and information is not compromised. It wants to be a leader in Cyber Security best practice – acting as an example for other London public sector organisations.

It does this through working closely with accredited, professional organisations (including our Cyber Security Partner and the National Cyber Security Centre). Using their expertise to provide informed guidance to the GLA and to assess the Cyber Threat environment. The GLA acts on their advice to ensure a robust, up-to-date, intelligence driven approach is adopted.

The approach is overseen by the GLA Governance Steering Board – with progress monitored by the GLA Chief Officer.

Responsibility for its delivery lies with the GLA Technology Group (A Senior Cyber Security Engineer leads on the Cyber Security Work that is built into the GLA's Digital and Technology Strategy and takes the lead in ensuring systems and services are robust).

The Technology Group work closely with:

- Teams that have responsibility for major systems (e.g. Social Media) to ensure that their systems and processes are secure.
- Organisational Delivery and Internal Communications Teams in ensuring a Cyber Security Awareness Culture is supported through accessible training resources, through staff induction and a regular emphasis on individuals' personal responsibilities in ensuring organisational security.

Threat Assessment

The GLA has recruited an NCSC approved, specialist Cyber Security Partner to assist the GLA in identifying the current and potential Cyber security risks facing the organisations like the GLA. They will provide regular advice which will be incorporated into the GLA's approach to keeping its cyber defences up to date. The partner will provide advice on configuration changes, policy and procedural changes and new tools (possibly including the further use of Artificial Intelligence) that may be required. This will also include identifying the use of other shared tools that might be available to the GLA. They will provide advice to the GLA on what international standards are appropriate for an organisation of the GLA's profile.

As part of the service they will undertake regular (6 monthly) detailed testing of our Cyber Defences (including all potentially vulnerable services including all GLA systems and infrastructure – including the use of social media) – providing feedback, based on this testing, about how further strengthening of our defences can be undertaken.

a) IT Strategy

Cyber Security is an integral and essential part of the Digital and Technological landscape at the GLA. Strong Cyber Defences are one of the five key aims of the GLA Technology Group – and this is reflected in the team's business plan. The GLA's Digital and Technology Strategy contains a programme dedicated to creating a secure environment to support cyber security.

b) Cyber Security Risk profile and posture

The key risks facing the GLA's information and technology infrastructure are set out in Section 4. The GLA faces a unique set of challenges in countering these threats whilst, at the same time, being an organisation that:

- Seeks to be highly transparent in the conduct of its business
- Require wide ranging access to internet-based information sources and services
- Is highly mobile, where staff have and need access to technology and digital services from multiple locations and devices.

In practice, it can be very difficult to do both to the highest levels of satisfaction. However, the balance will always be in favour of security whilst inconveniencing users to the minimum possible level. This will be achieved by adopting the following posture

Protect. Access to all data and systems, services and devices will be protected from unauthorised intrusion.
Monitor. All key technology services, systems and devices will be monitored continuously with alerting built in. Also, the cyber security threats facing the organisation will be regularly assessed.
Respond. All security incidents will be responded to, in line with the documented response plan. Where a new threat(s) emerges, respond to them by additional **Protect** measures.
Educate. Provide continuous awareness of good practice as well as mandatory regulations to GLA staff and ensure that all staff are complying with them through appropriate **Monitor** activities.

3. Outcomes

The outcomes sought from our Cyber Security Plan are to:

- minimise disruption caused by Cyber Security attacks
- promote best practice self-reliance for all GLA employees
- safeguard public money by reducing lost productivity
- consistently detect cyber security incidents so that action can be taken to prevent further incidents
- contribute to the delivery of the GLA's Anti-Fraud and Corruption Policy and Response Plan

The negative impacts arising from Cyber Security attacks that the GLA is seeking to avoid include:

- loss of resources (financial and other assets)
- defrauding of the GLA
- reputational damage

- damage to the GLA's relationships with partners and stakeholders
- disruption to service delivery
- outcomes not delivered
- legal action being taken against the GLA.

4. Scope and definitions

This policy is applicable to all Members, employees, temporary employees, external suppliers, contractors, and those to whom the GLA in general and Technology Group provide a service. The policy must be used to assess third-party suppliers who sign a contract to provide business services to the GLA. This policy must also be used to assess the risk of conducting business with those 3rd party providers. In accordance with GLA policy and procedures, this policy is reviewed and adjusted as needed on an annual basis or more frequently.

This policy defines Cyber Security as technologies, processes and controls designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects against the unauthorised exploitation of systems, networks and technologies.

It is increasingly important because the costs of data breaches are growing, cyber-attacks are growing in numbers and becoming more sophisticated. The policy seeks to ensure that proven best practices protect the GLA from Cyber Security attacks.

This GLA Cyber Security framework applies to the Mayor and to all staff and Assembly Members.

This policy defines Cyber Security as technologies, processes and controls designed to protect systems, networks and data from cyber-attacks. Effective cyber security reduces the risk of cyber-attacks and protects against the unauthorised exploitation of systems, networks and technologies.

It is increasingly important because the costs of data breaches are growing, cyber-attacks are growing in numbers and becoming more sophisticated.

The policy seeks to protect the GLA from the following Cyber Security Threats.

a) Ransomware

Which is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

b) Phishing

Which is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.

c) Malware and other electronic attacks

Which is any software or attacks by other electronic means intentionally designed to cause damage to a computer or network or steal GLA data.

d) Social engineering

Which is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes

5. Approach

Robust cyber security involves implementing controls based on three pillars: people, processes and technology. This three-pronged approach helps organisations defend themselves from both organised attacks and common internal threats, such as accidental breaches and human error.

a) People

The commitment to Cyber Security starts at the very top of the organisation and is reinforced as part of induction arrangements for Members and staff.

An e-learning module is available to all staff on the Intranet covering all aspects of Cyber Security. The current learning and awareness will be continually refined and enhanced through monitoring the cyber security and threat landscape.

This is also reinforced through messages in London@work, blog posts and on the Cyber Security Intranet pages

b) Processes and Technology

The GLA provides up to take security software and protection – including multi-factor authentication (where a code is sent to an app on an individual's phone) to reduce the possibility of accounts being hacked.

The GLA will ensure that software is kept up to date to ensure it has the latest protection against viruses and malware

The GLA will ensure that data is regularly backed up so that it is possible to recover from a ransomware attack.

The GLA will introduce additional protection to USB drives to keep GLA data safe if they are lost or stolen.

c) Monitoring and review

The GLA's Cyber Security framework will be kept under review to ensure it is working effectively and opportunities for preventing and detecting cyber threats are maximised.

In addition, this Policy and the Response Plan will be reviewed and as necessary updated at least every two years.

6. Responsibilities

Following are the GLA's information security roles and responsibilities:

Head of Technology Group

- provides governance for enterprise IT systems and information with respect to security compliance with this policy.
- ensures that the infrastructure standards incorporate security policies.
- provides guidelines for on-and-off network information systems with respect to maintaining an information security plan complying with the GLA's security policies.
- is accountable for effective Cyber Security practices at the GLA
- raising awareness and highlighting best practice in cyber security to limit the risks

Senior Cybersecurity Lead

- acts as primary custodian of the information security risk assessment process.
- reports identified risk to the enterprise risk committee and other key stakeholders.
- regularly updates the enterprise security policy and procedures.
- ensures identified system vulnerabilities are mitigated in a timely manner.
- publishes up-to-date security standards.
- acts as the incident lead during an active incident and is responsible for submitting a root cause report after the fact to the management.
- enforces compliance with enterprise security policies by conducting periodic security checks and audits.
- oversees internal and NIST CSF requirements.
- implements social engineering and other cyber security training campaigns
- supports due diligence process for vetting security quality of suppliers, products and services during procurements and shared service initiatives.
- assessing and making recommendations to improve the system of internal control
- reviewing, identifying and making recommendations to address risks associated with Cyber Security

Managers (All GLA\MOPAC\OPDC etc.)

- comply with the GLA's security policies by incorporating security practices, standards, and guidelines and incorporate them into the relevant procedures and processes in their teams.
- ensure annual security training is completed by the employees and non-employees (such as subcontractors and suppliers).
- disseminate relevant information and updates relating to Cyber Security
- act as role model for their team encouraging a culture of best practice
- follow established incident reporting and escalation procedures.
- ensure compliance with applicable enterprise policy and procedures (including ensuring the Technology Group are informed when individuals leave so that their accounts can be closed down)

Executive Director of Resources (statutory Chief Finance Officer)

- act as the GLA's champion for effective Cyber Security practices

Employees

- comply with the GLA's security policy and procedures.

- complete the security training as required.
- follow established incident reporting and escalation procedures.
- take care to protect their GLA equipment, data and access credentials.

Contracted third-parties, suppliers, temporary employees, and consultants

- must demonstrate they can meet and perform per enterprise policy and procedures.
- provide the GLA with required third-party audit reports as part of procurements

7. Policy Guidance by Functional Area

This cybersecurity policy covers the following functional areas:

- Cybersecurity
- Network Security
- Application Security
- Endpoint, Server, and Device Security
- Identity, Authentication, and Access Management
- Data Protection and Cryptography
- Monitoring, Vulnerability, and Patch Management
- High Availability, Disaster Recovery, and Physical Protection
- Incident Response
- Asset Management and Supply Chain
- Policy, Audit, E-Discovery, and Training

7.1 Cybersecurity policy guidance

The following subsections provide cybersecurity policy guidance for the GLA organised according to the preceding 11 functional areas.

The System Engineer is a critical function that oversees the management of sensitive enterprise information
System activities must include the following:
All systems engineer activities at the application, data, and operating system levels shall require authentication, and all logons to these systems shall be logged for audit.
Systems administration protocols that are insecure or vulnerable to attack, including critical infrastructures of storage, computing, and data centre management, shall only be used on isolated networks.
Systems administration accounts shall require multi-factor authentication before administrative access is granted.
Systems administrator activities shall be monitored for signs of inappropriate activity, and such signs shall be investigated within seven days of the occurrence.
Systems administrator logons shall be recorded and audited weekly.
Systems administrator access control lists shall be verified quarterly to ensure least privilege and separation of duties.
All changes to systems administrator access control lists shall be recorded and audited regularly in line with business security.
Systems administration security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.

Systems administration preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.2 Network Security

GLA access to the Internet may expose GLA's information systems, information and digital assets to other Internet users around the world. It is critical to protect the data and information systems from both internal and external malicious actors.
Network security activities must include the following:

- Network and network security infrastructure, including routers, switches, firewalls, and other components, shall be centrally managed and all logons shall be logged for audit.
- Network infrastructure administration activities shall be isolated from general business network traffic, and all administrative logons shall require credentials and multi-factor authentication.
- Networks that are publicly accessible or not physically protected, such as wireless networks and network connections in public spaces and conference rooms, shall use access control to ensure that only authorised users are permitted access.
- Networks shall have measures in place to detect and block network traffic that is known to be malicious, either through its protocols, its payloads, or its sources or destinations.
- Network traffic that is known to be malicious, either through automated or manual means, shall be blocked within one business day of detection.
- Access to GLA's networks from the Internet shall require multi-factor authentication. Access to privileged internal networks directly from the Internet shall not be permitted.
- Network traffic that is questionable and may be indicative of attacks shall be recorded and retained for 90 days to permit analysis and investigation after the fact.
- Secure network traffic shall not be excluded from analysis to identify and block malicious activity.
- Network infrastructure shall provide for basic services, including name service, host configuration, and time synchronisation, and these services shall be hardened to protect them from attack or compromise.
- Network configuration changes shall require approval and shall be logged for audit and investigation, as required.
- Network security configurations shall be reviewed on an annual basis, and all network policy configurations and exceptions shall be re-validated annually.
- Network security preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.3 Application Security

Enterprise applications are vulnerable to attack from the Internet and attackers with insider access. Vulnerabilities and mistakes in coding and deployment of application systems are also factors. The enterprise must protect these systems from attack and detect attacks and vulnerabilities in these systems when they occur.
Application security activities must include the following:

- Internet-facing application servers shall be protected from unauthorised configuration changes, and changes shall be logged and audited to catch the introduction of unauthorised "back doors" into these systems.
- Critical enterprise applications such as e-mail, voicemail, collaboration, and internal and external web services must be configured to prevent and detect attacks and exploits of vulnerabilities.

- For attacks and exploits that are not prevented or detected, adequate forensic logs must be maintained to permit audit and investigation after the fact.
- Communication between application components shall require authentication and shall be performed using secure protocols when performed over open networks. Where such protection is not feasible, network protection shall be utilised to protect these protocols and connections from attack.
- Applications that are sensitive to confidentiality concerns—processing data that is sensitive to breach—shall employ protection and detection to protect against data leakage.
- Applications that are sensitive to integrity concerns—potential data changes with financial or other repercussions—shall employ data integrity protections such as digital signatures and data modification audit trails to protect and detect against data changes.
- Applications that are sensitive to availability concerns shall employ high availability and rapid disaster recovery to protect them from denial of service attacks originating internally and from the Internet.
- Applications using custom source code shall have that source code analysed using static code analysis at least quarterly, and all medium and higher vulnerabilities shall be addressed or remediated.
- Applications that are generally available on the Internet or enterprise internal networks shall be scanned for vulnerabilities using a credentialed vulnerability scanner monthly, and all medium or higher application vulnerabilities shall be addressed or remediated within 90 days of discovery.
- Applications that are found to be in violation of policy may be temporarily or permanently disconnected from the Internet and/or the enterprise network until the violation is remediated.
- Application security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Application security preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.4 Endpoint, Server, and Device Security

Endpoints such as desktops, laptops, mobile devices, servers, Citrix systems and other appliances must be hardened and secured using standard vendor recommended security guides/builds. Endpoint, server, and device security activities must include the following:

- Local administrator account passwords or keys shall be unique to each endpoint. Enterprise wide endpoint management capabilities shall be considered to be critical security infrastructure and given appropriate protections.
- Enterprise endpoints and servers shall be configured from master images that are configuration-controlled and protected from tampering, changes, or the introduction of unauthorised or malicious code.
- Network-connected endpoint systems shall be configured to forward security logs—including administrator logon and security component configurations—to a central infrastructure for logging and correlation.
- All portable and removable endpoints—including personal computers, laptops, and mobile devices—shall have their built-in and removable media encrypted so it cannot be accessed without proper authentication to the device.
- Endpoint systems shall be configured for investigation of cyber-incident by installing forensic tools and configuring security logs to meet the needs of incident investigators.
- Endpoint systems shall be configured according to vendor-approved security guidelines for secure operating system installation and operation.
- Endpoint systems shall include endpoint protection to block and detect malicious software and network connectivity, as appropriate to the security posture of the system. Endpoints involved

in high-security functions may be configured for more restrictive security than general-use endpoints.

- Endpoints and servers involved in operating or managing cybersecurity functions for the enterprise shall have application whitelisting installed and configured for maximum restrictiveness.
- Personal computers and mobile devices, when used for enterprise work, must include the ability to remotely delete enterprise data from the systems in the event of compromise. If this is not available, the system must include safeguards to ensure that enterprise data is not stored on the device in a persistent state.
- Security infrastructure endpoints shall include the ability to detect and alert on changes to security configuration files within one hour of them occurring.
- Servers directly connected to the Internet shall be scanned for operating system vulnerabilities using a credentialed vulnerability scanner monthly, and all medium or higher operating system vulnerabilities shall be addressed or remediated within 30 days of discovery.
- Endpoints found to be in violation of policy may be temporarily or permanently disconnected from the enterprise network until the violation is remediated.
- Endpoint server and device security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Endpoint, server, and device security preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.5 Identity, Authentication, and Access Management

Access to enterprise systems shall require unique network identities and authentication to systems shall use approved means. This access shall provide for unique identification of the user and non-repudiation of their activities. Accesses to data and systems shall be configured on an as-required basis according to need-to-know. Accesses and online identities that are no longer required shall be removed on a timely basis.

Identity, authentication, and access management activities must include the following:

- All production enterprise systems shall use centralised identity provisioning and de-provisioning, and centralised access management where possible. Cloud-based systems and Software-as-a-Service solutions used by the enterprise are subject to this policy as well as on premise systems.
- Identity systems shall be protected at the same or greater level as the sensitivity of the enterprise applications that they serve.
- Identity systems shall provide protective, detective, audit, and forensic controls governing all administrative changes to the identity system, all identity life cycle actions—including account provisioning, de-provisioning, and changes—and permission provisioning, de-provisioning, and changes.
- Identity systems shall alert on suspected attacker activities, including using privileged accounts on non-privileged systems and patterns of excessive logons or logon attempts that may be malicious.
- Digital identities that are no longer needed shall be de-provisioned within 180 days.
- Access permissions that are no longer needed shall be removed within 90 days.
- Identity systems shall support the protocols required for authentication and access control on enterprise systems, including on premise and cloud-based systems. This includes Kerberos, RADIUS, LDAP, X.509 certificates, and Security Assertion Markup Language (SAML).
- Multi-factor authentication shall be supported for access to enterprise systems and applications from untrusted networks such as the Internet, and for all uses of privileged systems administrator accounts on all networks.

- Authentication failures shall not reveal information about usernames, passwords, permissions, or authentication methods.
- Failed logons shall include a delay so that no more than five failed logons can be performed in one hour (this may be implemented by a one-hour block after the fifth failed logon). More than ten failed logon attempts on a single account shall generate an alert requiring investigation before the account may be used.
- Identity, authentication, and access management security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Identity, authentication, and access management preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

Password Policy

Passwords, when they are used for authentication, shall be subject to the following policy requirements:

- Passwords should be at least 13 characters long, and longer pass phrases containing spaces are encouraged. Passwords must contain uppercase, lowercase, and a number or a special character. (This complexity is to resist brute-force attacks; password length requirements will increase over time as computing power to crack passwords increases.)
- Passwords should not contain internal repetitions to allow them to meet length requirements (for example, PasswordPassword1).
- Passwords must not be displayed in clear text during the login process and user accounts will be frozen after 5 numbers of failed logon attempts.
- User passwords shall not be written down on paper or stored in unencrypted computer files.
- System account passwords shall be physically protected in a locked safe. If stored electronically on network-accessible systems, such storage shall be encrypted and access-controlled. If a single electronic system contains more than 100 system passwords, user access to it shall require multi-factor authentication.
- When passwords must be generated and transmitted, such transmission shall be by encrypted means, or given verbally over the telephone. Only one-time passwords may be transmitted over insecure channels.
- Password security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Password management preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.6 Data Protection and Cryptography

Data protection and cryptography are essential to achieving strong authentication, non-repudiation, and the protection of confidentiality and integrity of data at rest and in transit. These capabilities are to be used to ensure enterprise data and identities are protected adequately to resist current and projected attacks. Data protection and cryptography activities must include the following:

- Sensitive data transmissions shall be protected using Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPSec), or equivalent secure protocols—on both internal protected networks and insecure networks such as the Internet.
- Encryption modules, algorithms, and protocols shall meet US National Institute of Standards and Technology (NIST) requirements as documented in approved Federal Information Processing Standards (FIPS) documents. Not necessary but implemented

- Cryptographic algorithms shall either be rated to resist brute-force attack for a period of ten years at the time of use by an attacker with worth of computing capacity or attempts to brute-force attack the cryptography shall be detectable.
- Published cryptographic vulnerabilities (such as Heartbleed) shall be remediated within 30 days of publication or compensating preventive or detective controls shall be put in place so that attempted exploits are blocked or at least detected.
- Encryption keys shall be centrally escrowed and retained for a period of seven years after the date of last use. This approach supports investigations by enterprise security, legal, or law enforcement personnel.
- All non-public enterprise data at rest shall be either physically protected in a locked facility or container or encrypted using cryptographic keys that are separate from the data (such as a strong password or encryption token).
- Data encryption shall include adequate logging separate from the media itself to permit investigators to validate that lost media was in fact encrypted at the time of loss.
- Strong and multi-factor authentication shall use cryptographic methods to make authentication resistant to keylogging, replay, session hijacking, and brute-force attacks. These methods shall include digital certificates, one-time passwords, and secure cryptographic modules for storing persistent private asymmetric and shared symmetric keys
- Persistent keys used for strong authentication or persistent encryption shall be protected using Hardware Security Modules (HSMs), Trusted Platform Modules (TPMs), secure elements, or smart cards that resist physical and logical attack to extract the keys.
- Session encryption (such as that used by SSL, TLS, or IPSec) does not require hardware protection, except where session compromise would pose an enterprise risk.
- Data protection and cryptography modules, algorithms, protocols, and security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Data protection and cryptography preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.7 Monitoring, Vulnerability, and Patch Management

Monitoring of account activity and security incidents relies on robust logging of activities and alerting that catches potentially malicious activities. In this way, the enterprise will be able to detect violations of security policies or procedures, and active attacks when they occur. Timely detection of malicious activities aids in preventing or containing malicious actions before damage can be performed. Vulnerability and patch management reduce exposure to attacks by tracking and remediating vulnerabilities in a timely fashion, and by patching systems to reduce their exposure to attack.
Monitoring, vulnerability, and patch management activities must include the following:

- Enterprise systems and cloud services delivering business-critical functions shall be monitored for performance and availability so failures can be detected within at least 30 minutes of their occurrence.

- Enterprise systems and cloud services shall forward their logs to a central system for correlation and analysis or shall provide for in-place analysis and alerting that ties in with enterprise incident detection and investigation services.

- All log entries shall be synchronised to Coordinated Universal Time (UTC) or a clearly delineated global time zone so the times when events occur are clearly presented to investigators.

- Security audit logging must clearly tie user activity in the information system to named user or service accounts.
- Security audit logs must be protected from tampering and shall be made available to support investigations for a period of one year after the event is logged. Event logs related to public company financial activities shall be retained for a period of seven years after the event is logged.
- Networks shall be monitored to detect rogue or malicious devices connecting to them, and wireless networks shall be configured to detect attacks and rogue wireless access points.
- Cybersecurity may use detective technologies such as endpoint detection and response (EDR) and SIEM to detect attacker exploits of vulnerabilities and identify attacker Tools, Techniques, and Procedures (TTPs).
- System security monitoring shall feed into a central system for correlation that is monitored 24x7 to detect security incidents. Security logs shall be monitored for activities known or suspected to be malicious. Security alerts shall be generated within 30 minutes of such activity occurring.
- New applications and servers shall be vulnerability-scanned, and all medium or higher vulnerabilities shall be addressed prior to becoming operational.
- Enterprise applications that are generally available on the Internet or enterprise internal networks shall be scanned for vulnerabilities using a credentialed vulnerability scanner monthly, and all medium or higher application vulnerabilities shall be addressed or remediated within 90 days of discovery. For sensitive systems with significant business impact, this remediation window may be shorter – as little as one day.
- Servers directly connected to the Internet shall be scanned for operating system vulnerabilities using a credentialed vulnerability scanner monthly, and all medium or higher operating system vulnerabilities shall be addressed or remediated within 30 days of discovery. For sensitive systems with significant business impact, this remediation window may be shorter – as little as six hours.
- Cybersecurity shall ensure that applications and systems in violation of vulnerability remediation policy shall be disconnected from the Internet and enterprise networks until remediation is performed and validated.
- Vendor-provided patches shall be evaluated and installed as recommended by vendors. Vulnerabilities relating to missing patches shall be handled as per vulnerability policy above. When security patches cannot be installed for operational reasons, mitigating preventive and detective controls shall be employed to keep the overall risk acceptable.
- Patching is the responsibility of the system owner. System owners may use automated systems to simplify patch deployment, but limitations in these systems must be compensated for using manual techniques to ensure that security vulnerabilities are addressed in a timely manner.
- Detective controls shall be configured to detect attacker exploits of known vulnerabilities when this is technically possible.

- Internet-facing and user networks shall be penetration-tested on an annual basis to identify vulnerabilities related to real-world attacker techniques.

- Monitoring, vulnerability, and patch management security configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.

- Monitoring, vulnerability, and patch management preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.8 High Availability, Disaster Recovery, and Physical Protection

GLA IT services, systems, and data shall be protected from losses of availability related to system failure, physical destruction, and accidental or malicious incidents. Services, applications, and servers shall be configured with adequate redundancy and protection to meet business needs and ensure cost-effective service delivery in the event of accidental or deliberate incidents targeting their availability.
High availability, disaster recovery, and physical protection activities must include the following:

- Availability: Business IT systems must have at least 99.9% availability. Supporting infrastructure may be subject to higher availability requirements as needed by the business.

Recovery Point Objectives (RPO) in the event of natural or man-made disaster:

- Business financial systems must be able to recover all committed transactions with customers or vendors that have financial consequences.
- Other business IT systems must be able to recover data up into the day previous to the incident (daily backups).

Recovery Time Objectives (RTO) in the event of natural or man-made disaster:

- Revenue-generating business functions must be able to recover and achieve initial operating capability within seven days.
- Business financial systems must be able to recover to initial operating capability within 45 days.
- Other business IT systems must be able to recover to initial operating capability within 90 days.
- RTO planning shall consider the time required for rebuilding affected servers, in addition to the time required for restoring affected data.
- Major system upgrades and configuration changes must include adequate backups to "roll back" the changes within the availability, recovery point, and recovery time requirements, as previously specified.
- Backup data shall be sufficiently protected physically and logically so that natural or man-made disasters will not result in the destruction of both the primary copy and the backup.
- Backup data taken offsite shall be encrypted, and the keys to that data shall be sufficiently protected from loss or compromise so that data can be recovered even in the event of catastrophic loss.
- Theft or loss of any enterprise-furnished equipment must be reported to the incident response team as soon as possible.

- Enterprise sensitive data printed on paper or other material must be physically protected in a locked room or cabinet.
- Enterprise facilities and data centres shall include physical protection, monitoring, and detective controls to protect personnel and equipment from harm and accidents. Sensitive data and systems handling it in unencrypted fashion shall be protected using double-barrier protection and need-to-know access controls.
- Any third-party access to the facility must be approved by the data centre operations supervisor and guests must be escorted during the visit.
- When automated physical access controls are used at enterprise facilities, the access logs shall be maintained for one year to support investigations by audit, security, legal, and law enforcement personnel. Logs shall be monitored 24x7 to detect intrusions and intrusion attempts.
- Backup media, replication processes, and snapshot procedures must be tested annually to verify their proper operation.
- Disaster recovery and service continuity plans must be tested using a drill, rehearsal or tabletop practical exercise every two years to ensure their effectiveness.
- Physical security risk assessments must be conducted for all data centres, server rooms, and server closets on an annual basis.
- High availability, disaster recovery, and physical protection configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- High availability, disaster recovery, and physical protection preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.9 Incident Response

A security incident is any malicious event (perceived or real) performed against the enterprise's data or information systems. An incident can originate inside the enterprise (insider threat), in external entities, or in the surrounding environment. When a cybersecurity-related incident is reported, the incident response team takes charge of the incident and matrixes in the appropriate resources from elsewhere in IT and the business to investigate and remediate the situation.
Incident response activities must include the following:

- The incident response team shall track cybersecurity threats against the enterprise and inform cybersecurity and IT leadership of threats that pose new or previously unknown risks to the enterprise and potential mitigations for those risks.
- All information systems supporting enterprise business processes must have a documented incident response process. Incident response processes must have clearly defined roles and responsibilities. These processes may include leveraging shared services for incident response that are centrally operated by cybersecurity.
- For major incidents, a single leader must be designated for the duration of the incident, from initiation through conclusion. The incident leader is responsible for coordinating containment of the incident, reducing the impact, ensuring remediation, and keeping all the stakeholders informed of status.
- Suspected incidents shall be investigated according to the following schedule:
- Alerts rated "critical" shall be investigated within one hour of their detection.
- Alerts rated "high" shall be investigated within 12 hours of their detection.
- Alerts rated "medium" shall be investigated within 24 hours of their occurrence.
- Alerts rated "low" or "routine" shall be investigated within two business days of their occurrence.
- All incidents shall be documented to capture the originating alert or event, results of investigation, and remediation and conclusion. Confirmed incidents shall have their root cause investigated, identified, and documented. Incident documentation shall be retained for seven years following the conclusion of the incident.

- Incident investigation teams shall have the tools and permissions they need to investigate accounts, computers, and networks involved in malicious activity. They shall have the ability to directly or by request disable and remediate accounts, computers, and networks as necessary to contain and resolve the incident.
- The cybersecurity department shall be responsible for overseeing contractual, regulatory, or legal obligations related to incidents; identifying incidents with contractual, regulatory, or legal implications; and bringing to bear the appropriate resources to ensure that contractual, regulatory, and legal obligations related to those incidents are met.
- The enterprise shall have anonymous methods for employees to report security policy violations or suspected security incidents without fear of reprisal.
- Incident response configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Incident response preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.10 Asset Management and Supply Chain

Asset management is accounting for all the assets (hardware and software) in the enterprise. It is critical that this information be kept up to date to support IT operation and handling of cybersecurity incidents. A supply chain management program covers both products and services to include security assessment, periodic re-assessments, and inclusion of supplier information in the asset management database.

Asset management and supply chain activities must include the following:

- All software and hardware assets shall be assigned to an enterprise system with a primary and alternate employee point of contact.
- A centralised asset management system shall be utilised to track all enterprise hardware and software assets from their acquisition through to their disposal.
- A centralised configuration and change management system shall be utilised to track configurations of enterprise hardware and software systems, track the approval of changes to those configurations, and detect unauthorised changes when they occur.
- Software licenses and software utilisation in the enterprise shall be tracked so that software licenses can be matched to utilisation, software license compliance can be ensured, and unauthorised software in the enterprise can be identified and remediated.
- As part of system acquisition, vendors and suppliers shall be reviewed and approved by cybersecurity, with associated risks identified and accepted, remediated, or mitigated.
- Hardware and software assets retired from service shall be properly disposed of, including the following:
  - Removal of assets from asset and configuration databases
  - Release of software licenses and termination of software and hardware support contracts
  - Sanitisation or destruction of hardware persistent storage (flash and hard drive storage) to protect enterprise data
  - Persistent storage media, including flash drives, portable media, hard drives, and device embedded storage (such as copiers and voicemail appliances with data storage features) shall be sanitised of enterprise data using physical destruction, data cleaning, data scrubbing, or data encryption methods such that the data may not be recovered after disposal.
- Data disposal methods shall be validated annually to ensure their effectiveness. Data encryption methods shall be validated to ensure the encryption strength is adequate to protect data for a period of ten years following disposal.

- Loss or unintended disposal of equipment or disclosure of data shall be reported as a cybersecurity incident.
- Hardware and software assets shall be inventoried annually, with all associated points of contact validated and updated as necessary.
- Hardware, software, and service provider risk evaluations shall be reviewed and updated annually, or when changes occur that materially affect the security posture of such providers (such as cyber-incidents or breaches, mergers, divestitures, bankruptcies, or foreign acquisitions).
- Asset management and supply chain configurations shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Asset management and supply chain preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

7.11 Policy, Audit, E-Discovery, and Training

Security governance is paramount for the smooth functioning of the enterprise cybersecurity program. This includes the maintenance of enterprise cybersecurity policies, periodic audits of controls and protections, support for legal e-discovery activities, and training of cybersecurity personnel, employees, and contractors in proper cybersecurity practices and techniques.

Policy, audit, e-discovery, and training activities must include the following:

- GLA cybersecurity policy shall be approved by business leadership, with inputs from key stakeholders in the business leadership, legal, contractual, IT, and cybersecurity departments.
- A formal security forum shall be established to enable key stakeholders to discuss security matters on a regular basis and document policy changes or recommendations for enhancements.
- The GLA shall track cybersecurity risks and their potential consequences and shall report on those risks and their mitigation on a quarterly basis.
- The enterprise shall employ tools to provide overall cybersecurity governance, risk management, and compliance reporting so that all contractual, regulatory, statutory, and legal requirements can be met.
- The GLA shall comply with all contractual, regulatory, statutory, and legal requirements as they are stipulated, General Payment Data Payment (GDPR), Payment Card Industry (PCI), ISO27001 and NIST CSF. This may also include regulations relating to privacy of employee and customer data.
- The GLA shall comply with all requests for e-discovery originating from the legal department. All requests shall be documented, along with the extent of the data provided in response to the request. This documentation shall be retained for seven years.
- Exceptions to cybersecurity policies shall be documented, tracked, and re-certified on an annual basis. Exceptions that are not re-certified shall be removed and the policy enforced.
- The GLA shall ensure that personnel in positions of significant business and cybersecurity trust are appropriately vetted.
- The GLA shall ensure all employees receive annual training on cybersecurity concerns and obligations. Employees in positions of trust, including executives and systems administrators, shall receive additional training suitable to their roles, the risks associated with those roles, and their obligations to provide for additional protection of enterprise and customer data.
- The GLA shall audit *all* cybersecurity preventive, detective, audit, and forensic controls on an annual basis to ensure their proper design and operation.

- Policy, audit, e-discovery, and training programs shall be reviewed on an annual basis, including re-validation of all policy exceptions.
- Policy, audit, e-discovery, and training preventive, detective, audit, and forensic controls shall be verified and tested for proper operation at least annually.

8. Compliance

Compliance lapses or failures with this policy may result in disciplinary action, such as removal or limiting access to the systems, termination of employment or contract, or unfavourable remarks in the employee performance review. The failures could have legal or regulatory ramifications regarding national, local, or international law. Compliance with the policy is conducted through executing periodic assessments by GLA security, internal/external audits, or self-assessments.

Appendix A: Technology Group - Cyber Security Plan

1. Approach / Governance

The GLA has appropriate cyber security governance processes with clear lines of responsibility for cyber security.

- The Executive Director, Resources is the Senior Responsible Owner for Cyber Security for the Greater London Authority (GLA).
- The Head of the Technology Group is overall responsible for key operational services.
- The Assistant Director of Finance and Governance is overall responsible for data protection issues.
- The Cyber Security Policy is produced by the Technology Group and then approved by the Governance Steering Group

The GLA have appropriate management policies and processes in place to direct the GLA overall approach to cyber security.

- The GLA Change Advisory Board (CAB) and Technical Design Board (TDB) is a joint meeting held fortnightly and chaired by the Cloud Services and Operations Manager.
- Key technical policies relating to cyber security are owned by Cloud Services and Operations Manager and approved by the GLA Technology Design Board (TDB).
- Any changes to the IT system must be approved in a Change Control by the Change Advisory Board (CAB).
- The TDB/CAB meeting maintains a risk log of technical risks relating both to business change risks and external risks. The risk log is reviewed at each meeting and risks above an agreed

threshold are escalated to the Technology Group Management Team. Corporate-level risks identified by the Technology Group Management Team are escalated to the corporate risk log.

- The operations of IT services are described in AQAP (assured quality action procedures) operational procedure documents. The Technology Group Configuration Manager is responsible for the storage and review of this collection of documents. Different categories of AQAP are owned and updated by appropriate teams.
- Key data protection policies are owned by the Information Governance Manager.
- The GLA identify and manage significant risks to sensitive information and key operational services.
- The GLA understand and manage security issues that arise through the use of external suppliers and through the GLA supply chain.
- The GLA use GLA and G-Cloud standard contracts that include clauses relating to confidentiality and data security for assignments that grant enhanced access to GLA systems. Enhanced access in this regard means knowledge about GLA systems that goes beyond that which is publicly available and/or details about the specific system(s) on which the supplier is working.
- Furthermore, the GLA will require that suppliers with enhanced access to GLA systems shall hold a valid Cyber Essentials certificate.
- For any work involving GLA Sensitive information, a separate risk assessment will be carried out in accordance with the documented processing and storage requirements for the sensitive data.
- The GLA provide data protection and cyber security awareness training for all staff through a dedicated Intranet page.

2. Sensitive Information

The GLA handles certain sensitive datasets that require enhanced security for processing and/or storage that exceed normal security levels. These datasets are considered to be "Sensitive Information". The enhanced security provisions for individual datasets are recorded on a case by case basis for each dataset.

Key information about each Sensitive Information dataset is held in a standard template. The TG Configuration Manager is responsible for managing and periodically reviewing the overall collection of records about Sensitive Information datasets. The template for Sensitive Information datasets holds the following information:

- Description
- Service Owner
- Data Processing/Data Sharing agreement
- Why the GLA holds or processes this information
- Where the GLA holds the sensitive information

- Which computer systems or services process the sensitive information
- Security Constraints around data processing and data storage (formal and/or informal)
- The impact of the loss, compromise or disclosure of the sensitive information

3. Key Operational Services

The GLA identifies and catalogues key operational services.

Information about key operational services is held in a Configuration database. The TG Configuration Manager is responsible for maintaining and periodically updating this database. Information held in the database includes:

- The key operational service
- Dependencies on other IT services
- Dependencies on other non-IT services

4. Access to Sensitive Information and Key Operational Services

The GLA understand and continually manage access to sensitive information and key operational services.

Users are granted minimum access to IT services necessary for their role. The following extensions to basic access require additional authorisation:

- Remote access
- Access to team drives by non-team members
- Access to certain HR data
- The procedures for setting up New Starters are governed by Technology Group AQAP procedures.
- The GLA remove access from individuals when they leave a role or leave the organisation.
- The Leavers' process, providing guidance for leavers and managers, is posted on the GLA Intranet.
- IT user Accounts are periodically reviewed. Accounts that have not been accessed in the last 90 days are suspended and the manager is contacted to confirm whether the account is still required.

5. Protection of Sensitive Information and Key Operational Services

The GLA only provide access to sensitive information and key operational services to authorised users or systems that are properly identified and authenticated.

Access to Sensitive Information is regulated by the data processing and storage agreement relevant to the specific sensitive information data set. This may include restricting access by IP address or device, or other restrictions such, for example, regarding the handling of backups.

The GLA operates the Principle of Least Privilege providing only the minimum access necessary to services and data.

Users and systems are always identified and authenticated prior to being granted access to information or services. Multi-Factor Authentication (MFA) is required for access to services and user data when working away from a GLA office.

Additional restrictions may be required for access to Sensitive Information datasets, depending on the agreement regulating the processing and storage of the specific dataset.

6. Protection of GLA Systems

The GLA protects its enterprise technology by:

- Tracking and recording all hardware and software assets and their configuration using a range of different technologies
- Ensuring that infrastructure is not vulnerable to common cyber-attacks. This is achieved through fully automated patching, and manually initiated automated patching. There is a separate Windows Server Patching Policy.
- Undertaking annual perimeter testing to test for known vulnerabilities and common configuration errors. The GLA will also undertake annual internal security testing.
- Ensuring that changes to the authoritative DNS entries can only be made by strongly authenticated and authorised administrators
- Maintaining an up to date IP scoping document
- Maintaining information about outsourced and cloud services and the security-related responsibilities that remain with the GLA for each service

The GLA protects end user devices by:

- Accounting for end user devices using a combination of asset management software and security software.
- Adding extra technical restrictions to devices accessing Sensitive Information, if required by the policies governing access to the specific sensitive information dataset.
- Ensuring that operating systems and software packages are patched regularly in accordance with agreed policies. The GLA operates a cloud-first policy. Desktop services are being migrated to the cloud and will be automatically patched by the vendor when they are migrated.
- Encrypting data at rest when physical protection cannot be assumed. Encryption at rest will be enforced on mobile devices (e.g. Apple IOS and Android) and Windows 10 devices such as Surface Pros. Windows 10 laptops and Surface Pros will enforce a policy that removable media must be encrypted if information is being written to the media.

- The security of data at rest on mobile devices and removable media, and the management of mobile devices is governed by a separate Mobile Device and Removable Media policy

The GLA protects email by:

- Enforcing Opportunistic Encryption meaning that Transport Layer Security Version 1.2 (TLS v1.2) is used for sending and receiving email provided this is supported by the other party.
- Using Sender Policy Framework (SPF). The GLA is committed to using Domain-based Message Authentication Reporting and Conformance (DMARC) and Domain Keys Identified Mail (DKIM) on incoming and outgoing email.
- Implementing spam and malware filtering on inbound email.

The GLA protects digital services by:

- Ensuring that GLA web application are not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.
- Carrying out annual penetration tests and penetration tests on any significant new services added to the digital estate, testing that the hosting environment is secure, and testing for the presence of known vulnerabilities.
- Protecting data in transit using well-configured Transport Layer Security Version 1.2 (TLS v1.2)

7. Highly Privileged Accounts

The GLA will ensure that highly privileged accounts are not vulnerable to common cyber-attacks by:

- Ensuring that users with enhanced system privileges do not use their privileged accounts for high-risk functions such as email and web browsing.
- Carrying out a 6-montly self-audit declaration of those users with privileged accounts.
- Using multi-factor authentication where technically possible for administrative services that provide access to manage cloud-based infrastructure, platforms and services.
- Using multi-factor authentication for access to enterprise social media accounts
- Requiring that highly privileged accounts are changed from default values and are not easy to guess. Passwords which grant extensive access will have high complexity.

8. Detection of Cyber Incidents

The GLA takes steps to detect common cyber-attacks by:

- Capturing information and monitoring information about events by machine
- Participating in relevant cyber security networks
- Focussing monitoring on high risk areas in accordance to the Risk Log maintained by the GLA Technical Design Board. The Risk Log is reviewed at each meeting of the Technical Design

Board. Additional monitoring or safeguards may be brought into operation depending on the current risk profile.

- Maintaining a log of significant cyber security incidents
- Monitor digital services that are attractive to cyber criminals for the purposes of fraud. Such services and datasets will be included in the collection Sensitive Information. Appropriate safeguards regarding processing and storage will be put in place according to the specific requirements of the dataset or service.

9. Responding to Cyber Incidents

The GLA have defined, planned and tested response procedures for cyber security incidents by:

- Having in place an incident response and management plan for incidents relating to infrastructure or public-facing digital estate whether these incidents are security-related or operational
- Having in place a procedure for communications with senior management for incidents relating to infrastructure or the public-facing digital estate whether these are security-related incidents or operational
- The GLA Governance Team and/or the Senior Responsible Owner is responsible for communication with external agencies such as the Information Commissioner's Office.

The GLA have well-defined and tested processes to ensure business continuity in the event of system failure or compromise, by:

- Having in place a Disaster Recovery and Business Continuity plan to continue to deliver essential services in the event of any failure, forced shutdown, or compromise of any system or service.
- Periodically shutting down and restarting services to ensure that this is a well-practised scenario.
- Conducting Service Outage Review meetings following major incidents with specific, assigned actions to ensure that the same issue cannot arise again
- Periodically reviewing the Technical Design Board Risk Log in the Technical Design Board meetings