GREATER**LONDON**AUTHORITY

Cyber Security Policy & Response Plan

Issue Date	February 2019 (Issue 1.1)
Amendments from previous version	N/A first version
Approved by	Executive Director of Resources
Review Date	December 2020
Senior owner	Executive Director of Resources
Document owner	

Contents

Cyber Security Policy

1. Introduction

1.1 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 Greater London Authority 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.

1.2 The objective of cyber security is therefore to achieve and maintain a condition where all information, systems and networks are available at all times to those who are authorised to use them. Furthermore, that the data and information held by the Greater London Authority 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 Greater London Authority.

1.3 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

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

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

2. Outcomes

The outcomes sought from our Cyber Security Plan are to:

- minimise disruption caused by Cyber Security attacks
- promote best practise 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

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

- loss of resources (financial and other assets)
- 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.

3. Scope and definitions

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

Which is any software intentionally designed to cause damage to a computer or network.

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

4. 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.

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.

5. Responsibilities

Executive Director of Resources (statutory chief finance officer):

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

Information Technology:

- deploying effective cyber-security measures, raising awareness and highlighting best practice to limit the risk of phishing attacks and other forms of digital fraud

Internal Audit:

- assessing and making recommendations to improve the GLA's system of internal control

- reviewing, identifying and making recommendations to address risks associated with Cyber Security

All GLA staff:

- adhering to the policies referred to directly above.
- Using a complex password and not sharing it or using it for other non-GLA services
- Taking care with personal data and following the GLA's guidance on GDPR
- Taking care when dealing with emails – particularly when asked to open a file or click on a link

Contractors, funding recipients and partners:

- adhering to the GLA's policies referred to above.

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 desktop services and user data.

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