Information Security Policy

BIRMINGHAM
2022
commonwealth
games

December 2019

Document Control

Document Information

Document title:	Information Security Policy
Document author:	Chief Information Officer
Document reference number:	CPOL-TEC-002
Date reviewed by Senior Management Team:	10 December 2019
Date approved by OC Board	Not applicable
Date and outcome of Equality Impact Assessment:	18 August 2019 – No impact on any protected characteristics
Date document issued:	11 December 2019
Review date, if applicable:	Not applicable
Target audience: (e.g. all staff)	All staff and those with access to OC systems
Subject area: (e.g. Finance, HR, Legal)	Technology

Version History

Version No	Lead	Date change implemented	Reason for change
1	Chief Information Officer	Not applicable	No change – new document

Consultation History

Position	Organisation
Data Protection Officer	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Head of Venue Technology	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Director of Telecommunications and Technology	Birmingham Organising Committee for the 2022 Commonwealth Games Limited
Senior Enterprise Architect	Birmingham Organising Committee for the 2022 Commonwealth Games Limited

Disclaimer

This is a proprietary Birmingham Organising Committee for the 2022 Commonwealth Games Limited (the OC) document and is not to be relied upon by any person other than the OC and its staff and those who are expressly authorised in writing to rely on the contents of this document. The OC makes no express or implied guarantees, representations or warranties to any third party as to whether the requirements of this document will be fulfilled by the OC, its staff, agents, contractors, authorised representatives or anyone else to whom the document relates or refers. The OC accepts no liability for any reliance by any third party on the contents of or the procedures detailed in this document.

Copyright

Contents

Purpose

The Birmingham 2022 Organising Committee handles large quantities of information relating to Suppliers, Athletes, visiting Dignitaries, Officials, Spectators, and its own Workforce, as well as its internal business operation delivering the Games. This information may be accessible in several ways; both electronically and in hardcopy format.

Maintaining the safety and security of organisational data and systems is a key requirement for all workforce and users of OC systems. This policy describes the measures users are required to take to maintain the security of OC data.

1. Scope

This policy is relevant to all users of Birmingham 2022 systems and information including;

- Employees
- Volunteers
- Contractors

2. Objectives

The objective of information security is to achieve and maintain a condition where all information is available at all times to all those who need it, cannot be corrupted or disclosed to unauthorised persons and its origin is authenticated.

The objectives of the policy are to

- Ensure the appropriate protection of all important and sensitive Birmingham 2022 information assets and services.
- Provide management direction and support for achieving compliance with this policy.
- Ensure data confidentiality is maintained and information is accessible when required to appropriately authorised persons.
- Enable consistent application of security controls across Birmingham 2022.
- Enable awareness of required technical controls, for example firewalls and procedures for employees, volunteers and contractors.
- Reduce operational, business and legal risk.
- Ensure compliance to relevant legislation and statutory guidelines.

Compliance with this Information Security Policy is necessary to ensure business continuity, and minimise business damage by preventing the occurrence, and minimising the impact, of information security incidents.

3. Definitions

3.1 Information Asset

An information asset can be described as any piece of information, hardware and /or software that has a value to Birmingham 2022 and would have a risk associated to it should it be lost, disclosed or tampered with.

3.2 Employees

Birmingham 2022 paid, short-term paid, interns, apprentices and secondees.

3.3 Volunteers

Birmingham 2022 pre-Games volunteers and Birmingham 2022 Games-time volunteers.

3.4 Contractors

Birmingham 2022 consultants, embedded contractors, and work experience.

4. Administrative Responsibilities

4.1 Business Data Owner (BDO)

All information assets shall be owned by a named individual within the Functional Area (FA) who will have responsibility to ensure adequate security of information assets. There will be several BDO's as each functional area will have business systems and data specific to their area which will require management and ownership at senior management level.

BDO's will be defined at project initiation stage and will be the person who will be ultimately responsible for the data the functional area generates and stores on the Birmingham 2022 systems and/or applications provided to support the business function.

BDO's shall authorise users requiring access to information assets owned by them or delegate responsibility to defined individuals.

BDO's must have oversight of the functional area data requirements and the authority to carry out the responsibilities below:

- Defining the requirements for information asset availability;
- Defining the classification of the business information, ensuring a risk assessment is performed to ensure security controls are relevant and up to date;
- Defining the responsibilities of users processing data;
- Define storage areas for general and specific business data assets, including applications;
- Approving which data users may access and that user's privileges are appropriate for the job function;
- Ensuring the systems that contain the information asset comply with this Information Security Policy;
- Informing the SA (System Administrator) when a user's access rights need to be created, amended or deleted, including the actions to be taken with respect to any personal data remaining on Birmingham 2022 systems;
- Ensuring appropriate copyright and license agreements are adhered to; and
- Ensuring that legal (including Data Protection) and contractual requirements are adhered to.

4.2 System Administrator

System Administrators (SAs) are generally technical / system administrators of the systems used to supply the applications and services, with responsibility for the provision of security controls required to protect the information asset. The SA may be an employee of Birmingham 2022 or from a third party.

NB: Where a third party is a data processor there will be a requirement for the BDO to be responsible for this relationship.

The System Administrator's responsibilities include:

- Ensuring compliance of the Information Asset with the Information Security Policy;
- Maintaining records of compliance to the Information Security Policy for future audit requirements;
- Interpreting and applying the Business Data Owners defined security control requirements;
- Ensuring backups and archives are created and secured according to policy; and
- Monitoring and reporting security incidents to the Business Data Owner and Information Security at email address: Andy.Peacock@birmingham2022.com.

4.3 Executive Management Team (EMT)

The EMT shall be accountable for ensuring that appropriate security, legal and regulatory controls are identified, implemented, and maintained by BDOs. They shall be supported in this task by all employees and provide appropriate resources to maintain compliance with this Information Security Policy.

BDOs within the EMT shall be responsible for the identification, implementation and maintenance of controls that are commensurate with the value of the information assets they own and the risks to which they are exposed.

4.4 IT Security Manager

The IT Security Manager (Technology) has direct responsibility to the Chief Information Officer for maintaining this Information Security Policy, providing advice and guidance on its implementation and managing information security at an operational level.

4.5 Data Protection Officer (DPO)

The Data Protection Officer has a statutory duty to monitor internal data protection compliance, provide advice on data protection obligations and Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner’s Office.

4.6 All Employees, Volunteers and Contractors

All Employees, Volunteers and Contractors shall adhere to this Information Security Policy.

Non-compliance with the Information Security Policy will be treated as an incident and reported as such to an individual’s line manager.

Any incident that results in loss or compromises OC data or systems should be reported to the IT Security Manager and the DPO immediately upon discovery.

5. User Access Control

Access to information assets shall be restricted to authorised users only and shall be protected by appropriate physical and logical authentication and authorisation controls.

Individual access to premises, systems, services, or information shall be determined on a Need-to-Know basis and in accordance with business requirements.

Password issues, resets and unlocks for sensitive accounts (where access is granted to personal data or confidential information) shall undergo an identification and verification process.

5.1 User Access Privileges, Creation, Modification & Termination

- Access privileges shall be allocated to users based on the minimum privileges required to fulfil their job function.
- Access privileges shall be authorised by the appropriate BDO.
- All access permissions shall be requested via the Service Desk.
- The Starters, Leavers and Movers process shall be documented and used for creating, terminating, modifying or revoking a user's access in a timely manner.

5.2 Access to Special Privileges

- All access to high level privileges (i.e. Domain Administrator in Windows operating systems, System Administrator for Finance and HR systems) shall be controlled using a formally documented procedure and access to the passwords for these accounts will be monitored.
- Special privileges are obtained by separate accounts from normal user functionality. The password to this account is controlled by a password management system. These accounts shall be formally controlled and access shall be provided to the minimum number of individuals and reviewed quarterly by the IT Services Department.
- Privileged individuals shall be instructed to use strong passwords and not to use their administrative access to setup new user accounts, or amend existing accounts, outside the formal documented processes for account creation and modification.

5.3 Password Management

All passwords used to access information assets shall conform to Birmingham 2022 requirements relating to password composition, length, expiration and confidentiality.

The approach to password management shall ensure:

- passwords are at least eight characters long.
- passwords contain at least two alphabetic characters and two numeric or special characters.
- passwords are required to be changed on first use and then every 90-days.
- privileged accounts shall have their passwords changed immediately after use.
- passwords can only be changed after successful authentication by the account owner.
- passwords shall not be the same as the last six previously used.
- passwords are not displayed when being entered.
- password files are stored separately from the main application system data.
- passwords are only stored in a hashed form.
- passwords are not recorded in audit trails.
- default vendor passwords are changed following installation of software.
- accounts will be locked out after a maximum of five invalid logon attempts.
- locked accounts remain locked unless line manager approval is given to unlock them.
- passwords are to be re-entered to unlock accounts that have been inactive for a period of more than 10 minutes .

5.4 Operating System, Network, Application and Remote Access Control

- Individuals wishing to access systems, services or components within the corporate network are required to provide unique and valid credentials to an authentication mechanism.
- Security and access control mechanisms to segregate networks into logical domains shall be deployed.
- Remote users, including third parties, shall use two-factor authentication when connecting to the network.
- Where third parties support or maintain any elements of the corporate systems or infrastructure that may be used to store, process or transmit user data, suitable contractual arrangements shall be put in place to require the third party to comply with the Organising Committee Policies
- All third-party access to the corporate networks and systems shall be reviewed regularly.
- Encrypting the transport of data, such as the use of a VPN or TLS (minimum version 1.2), must be deployed where there is a requirement for a system to communicate with a remote system and where that communications channel traverses a public network or a third party private network.

5.5 Access Right Audits

- All access rights shall be reviewed by the Business Data Owner (with the assistance of the Service Desk) at a frequency consistent with the business risks but on an annual basis as a minimum. For Critical systems, this audit will take place at least quarterly.
- A monthly audit identifies accounts that have been inactive for a month; the relevant BDO is asked to review these before removal.

5.6 System Monitoring, Logging, and Auditing

- Corporate networks and services shall incorporate tools for real-time monitoring, measuring and reporting of the performance of the service and to detect unauthorised activity.
- Monitoring systems shall provide at least three months of data immediately available for review.
- Quarterly network security reviews shall be scheduled to identify any risks that may arise over time and ensure agreed levels of service and control.
- Independent third-party vulnerability scans against internal and externally facing corporate systems and networks shall be conducted.

6. Network Security

6.1 Technical Controls

- The Birmingham 2022 internal networks shall be protected using firewalls and other appropriate detection and prevention systems.
- Network administrators shall establish appropriate controls to ensure the security of data in networks, and the protection of connected services from unauthorised access through effective access control, patch management, intrusion detection systems and virus prevention.
- A consistent set of network management procedures shall be applied across all corporate networks and infrastructure.

- Permission must be gained before any system or device is connected to the network.
- Operational responsibility for networks shall be separated from computer operations.
- Responsibilities and procedures for the management of remote equipment, including equipment in user areas, shall be established.
- Special controls must be established, based on a formal risk assessment, to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems.
- Computer and network management activities shall be closely coordinated, both to optimise the service to the business and to ensure that security measures are consistently applied across the organisation.
- Secure wireless access to the corporate network will also be provided.
- Any system connecting to the corporate wireless network will be subjected to an automated assessment to confirm they are running:
    - Up to date Anti-Virus.
    - The Windows Firewall is activated.
    - They have been joined to the Birmingham 2022 domain.
    - Hard disk encryption process is active.
- A guest wireless network may also be provided with separate access from the corporate network. Access will require a password.
- All Wireless Access Points (WAP) shall be protected from unauthorised physical access, configured with a minimum of WPA2 (Enterprise Mode) encryption, with default pre-shared keys changed.
- A hardware inventory asset register shall be maintained that records all WAP devices.
- All third-party access to OC network shall be authorised by an appropriate Business Data Owner (BDO) and, if necessary, monitored. BDOs shall specify access timeframes and be prepared to offer justification for such access, considering business need and identified risks.

6.2 Operational Management

- The network owners shall monitor network activities.
- All changes to the network shall be documented and authorised through a Change Control process.
- An inventory of network assets shall be maintained and all cables / patching sockets shall be correctly labelled and identified.
- All network security devices shall be configured to follow a 'least privilege' policy, such that any network traffic that is not explicitly allowed shall be explicitly denied.
- All devices connected to the network shall ensure they are configured as per the individual requirements of their hardening standard. All firewalls, routers, switches shall be hardened such that minimum services are running and file system security is locked down.

6.3 Failure and Redundancy

- All network security devices shall be deployed with a 'fail safe' configuration such that should the appliance fail and in the absence of any failover / high availability infrastructure all network access shall be blocked, dropped, and/or denied.

- All hardware platforms and software running on them shall be maintained at current, supported and replaceable version levels.
- Appropriate fall back arrangements shall be established for each network service.
- All network equipment shall be protected against natural hazards, power failure and unauthorised access.

7. Cryptography and Encryption

Encryption (and cryptography in general) provides three types of protection: source authentication, integrity and confidentiality.

7.1 Key Management

Key management refers to the establishment of cryptographic keying material for use with a cryptographic algorithm to provide protocol security services, especially integrity, authentication, and confidentiality.

The entire security of any given key management scheme is dependent on the security of the keys and the effective implementation of an approved documented key management process for managing the full lifecycle of cryptographic keys – specifically:

7.2 Key Control, Maintenance, Usage and Sharing

- All B2022 employees whose job description requires that they handle and access cryptographic materials are to undergo formal screening on hire (to achieve SC clearance) and periodically thereafter in accordance with HR policies.
- Key custodians are required to sign a form stating they understand and accept their responsibilities.
- No individual shall have access to all components or access to clear (plaintext) keys.
- Keys encrypted under approved encryption algorithms may be considered secure, but must not be copied or taken off-site.
- Cryptographic keys must be delivered to their point of use in a timely and secure manner. Delivery systems should verify that the client system is entitled to use the subject key. Automatic key delivery systems enable keys to change at relatively short terms intervals and should be used wherever possible.
- Acceptable key strengths and algorithms shall be based on the latest NIST and ENISA guidance, as defined by the IT Services team
- All licences shall be obtained to export, import, and/or use products containing cryptography.
- Physical and logical controls shall protect all keys to ensure they are not compromised.

7.3 Use of Encryption

- Encryption shall be considered when sending any sensitive information outside the OC network.
- Passphrases shall be communicated over a different medium than the protected information.
- Any internet facing service requiring Public Key Infrastructure (PKI) shall use certificates signed by a Certificate Authority (CA) approved by the IT Services team and managed securely.

- All laptops must be encrypted.

7.4 Cryptographic Audit

- All access to cryptographic key materials must be auditable.
- A Key Management Auditor, someone not normally part of the key management process, should be appointed to provide independent scrutiny of key management log files. Any anomalies are to be reported and escalated as part of the Incident Report procedure for immediate investigation.
- A written record must be maintained for any manual access to cryptographic keys / key parts, whilst changes made to the Key Management workstation are to be logged electronically.

7.5 Key Compromise

- If there is a compromise (suspected or known) of cryptographic keys a procedure to replace and investigate must be followed:
- All instances of cryptographic key compromise (suspected or known) must be reported and recorded in accordance with the Incident Response processes.
- Each compromise must be investigated with a view to containment and prevention.

8. Information Security Risk Management (ISRM)

8.1 ISRM Approach

Information Security Risk Management (ISRM) is the process of managing risks associated with the use of information technology. It involves identifying, assessing, and treating risks to the confidentiality, integrity, and availability of B2022's information assets.

ISRM is not a one-off exercise with a single set of control recommendations which remain static in time but a continual process. During the operational delivery and maintenance of the Commonwealth Games there will be several instances where risk assessment activity will be necessary.

A systematic approach is necessary to identify business needs regarding information security requirements (including contractual and regulatory) and to create an effective operational security framework.

The implementation of the information risk strategy shall be based on formal methods for risk assessment, risk management and risk acceptance and will be independent of technology or software.

8.2 Approach to using Third Parties

The risks associated with engaging a third party will also need to be identified, assessed and managed. Where third parties are used to manage B2022 information or information processing facilities, a formal contract shall be in place which defines the information security requirements of the relationship.

The delivery of the contracted services shall be monitored, and formal procedures shall be put in place to manage change and the identification, reporting and management of information security incidents. All contracts with third parties shall provide the Executive Committee with the right to audit the third party.

8.3 Reporting of Security Incidents

If any employee suspects or has knowledge of a security incident or a breach of B2022 information security policies, procedures and guidelines, or a software malfunction, or a security weakness in any information system, they must report their concern immediately to their Line Manager. Examples of a security incident include but are not limited to:

- Loss or theft of B2022 equipment or sensitive data.
- Physical damage to B2022 IT equipment.
- Compromise of sensitive documents and information.
- Unauthorised use of another user's profile (masquerading of user identity).
- Divulging a password to another user without authority.
- Improper use of e-mail or the Internet, e.g. harassing e-mails, downloading or distribution of pornographic images.
- Unauthorised copying of B2022 information.
- Access to B2022 premises without authority, and
- Damage to B2022 property that could impact information security.

In order for B2022 to be able to manage and deal with security incidents successfully, all incidents will be captured and logged.

In all cases, the IT Security Manager is ultimately responsible for ensuring that the Security Incident Report Form (documented in Appendix) is completed with the help of the person reporting the incident, and where relevant, may seek input from other staff, e.g. HR, Technology, Physical Security or an appropriate Functional Area Manager.

9. Policy Monitoring

The IT Security Manager who is directly responsible to the Chief Information Officer, will monitor the implementation of this policy and any subsequent revisions. This will include:

- Monitoring incidents of lapses in Information Security with a view to making any necessary amendments to the content of this or other related policies and procedures;
- Monitoring concerns made by individuals regarding the policy or its implementation;
- Undertaking periodic reviews of workforce awareness of and adherence to the policy;
- Providing a single point of contact for information security policy.

10. Ongoing Policy Review

This policy will be subject to review biannually after its date of approval. Earlier review may be required if any of the following occur:

- The adoption of the policy highlights any errors or omissions in its content.
- Where relevant changes in legislation or national guidance impact upon the content of this policy.

11. References

- GDPR (General Data Protection Regulations) May 2018

- Security Incident Report Form