

Information Security Policy

Reference: GMICT P 0016

Publication: 1 February 2023

Version: 8.0

Effective: 1 February 2023

Purpose

To enable the Public Administration to uphold information security. It is aligned to **ISO 27001:2013** (Information technology - Security techniques - Information security management systems – Requirements).

Scope

The scope of this Policy includes:

- ICT devices and storage in use within the Public Administration
- ICT devices connecting to the Malta Government Network (MAGNET)
- Systems that maintain and process Government data
- Auditing of solutions containing and/or transmitting production data
- Electronic representations of data
- Classified data carrying a Security Marking of *Restricted* or *Confidential*, throughout an ICT Solution's lifecycle.

Definitions

Underlined terms are defined in the Vocabulary (GMICT X 0003).

Contents

Purpose	1
Scope	1
Definitions	1
General	3
Organisation of Information Security	4
Security Marking of Data	4
Physical and Environmental Security	4
Asset Management	6
Access Control	6
Account Management	8
Passwords	9
Protection of Production Data	10
Cryptographic Controls	11
Operational Procedures and Responsibilities	11
Protection from Malware	12
E-mail and Internet	12
Technical Vulnerability Management	13
Connecting to MAGNET	13
Servers	14
Backup and Restoration	15
Clock Synchronisation	15
Audit Data	16
System Acquisition, Development and Maintenance	16
Information Security incident management	16
Business Continuity Management	17
Information Security Reviews	17
Intellectual Property Rights	18
Acceptable Use	18
Account management for specific work life instances	19
Human Resource Security	20
Appendix 1: Security Marking List	21
Security Marking	21
Description	21
Preparation and handling	21
Access	21
Copying and Storage	21
Exchange	21
Archive or disposal	21
Deviations from GMICT Policy	25
Issuing Authority	25
Contact Information	25

General

1. Confidentiality, Integrity and Availability shall be the underlying security principles throughout a lifecycle of any Solution that handles Government data.
2. It is the responsibility of all relevant stakeholders (including contractors/suppliers) to maintain Government information security and contribute to it, in accordance with this Policy and other applicable Policies and/or procedures.
3. All relevant stakeholders shall be committed towards the continual improvement of information security.
4. Management shall facilitate training and awareness of Information Security and shall ensure that all relevant stakeholders (including contractors/suppliers) under their responsibility abide by the relevant security policies and procedures.
5. Management shall ensure that sufficient Information Security resources are made available.
6. Information Security is a shared responsibility. Stakeholders of a System shall be responsible for the Information Security of their respective artefacts.
7. The Data Owner shall adopt a risk-based approach for decisions and investment relating to Systems managing data for which they are responsible. The Data Owner is responsible for any residual risk that may not have been mitigated following the implementation of selected controls.
8. Security controls shall be applied to a Solution as agreed with the Data Owner.
(Refer to Implementation Guidelines below)
9. Groups of services and/or Systems shall be segregated based upon:
 - security requirements
 - the data's Security Marking
 - risk associated with the respective service and/or System
 - cost of segregation
 - resulting operational performance constraints
10. Multi-factor authentication shall be enabled for access to any Government ICT service provided by the Agent.
11. Handling of personal data shall comply with the [General Data Protection Regulation](#)¹, (EU) 2016/679 and any other applicable legislation or regulation.
12. Government organisations assuming the role of Identity providers and providing federated identity services shall:
 - a. As a minimum, be in line with the requirements of ISO27001:2013
 - b. Seek authorisation from the Agent².

Implementation Guidelines

For systems that are hosted on or connect to the Government corporate infrastructure, the Data Owner shall seek guidance from the Agent's Security and Governance function regarding security controls that shall be considered.

¹ <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1571925658226&uri=CELEX:32016R0679>

² Specifically through the Agent's Security and Governance function.

For services offered by the Agent, the Data Owner shall seek direction from the Agent's Security and Governance function regarding security controls that shall be implemented.

Organisation of Information Security

13. The Data Owner shall identify and allocate responsibilities for the protection of data and for carrying out specific Information Security processes.
14. The Data Owner shall ensure that conflicting duties and areas of responsibility shall be segregated to reduce risk of unauthorised or unintentional modification or misuse of Government data.
15. The Project Manager shall ensure that Information Security principles are part of all phases of a project.
16. Appropriate contacts with relevant security-related external authorities and special interest groups shall be established and maintained.

Security Marking of Data³

17. Handling of classified information is regulated by the Manual of Procedures for the Handling of Classified Information in the Malta Public Service.
18. The Data Owner shall assign a security marking to data for which they are responsible.
19. In the absence of the assignment of a security marking, the data shall be treated as *Unclassified* up to **29th January 2024**, whereupon, if still not assigned a security marking, the data shall be treated as *Restricted*.
20. The Data Owner shall ensure that any ICT Solution or ICT device used to capture, access, process, store or exchange data that has a continuing value to Government is secured from unauthorised access, modification or creation of data through the application of Security Controls commensurate with the Security Marking of such data.
21. Where possible, different parts of a System shall be assigned a security marking in a granular manner, according to the security marking of the data that each part captures, transmits, stores or processes. A System shall be marked based on highest security marking of data that it shall capture, transmit, store or process.
22. Any data and/or software residing on ICT devices and/or media that the Data Owner shall no longer be responsible for, shall be securely removed using a method commensurate with its security marking.

Physical and Environmental Security

23. Encryption shall be carried out on all workstations using the Agent's corporate solution as determined by its Information Security and Governance function. The encryption key may be stored in the Agent's central key repository. It is the responsibility of the end user to ensure, on a regular basis, that the key can be retrieved from the repository.
24. Storage, exchange, archival and removal of data shall be commensurate with the data's security marking.

(Refer to Implementation Guidelines below: a)

³ Refer to Appendix 1.

25. Authorisation from the respective Data Owner shall be sought prior to removal of equipment, data or software of a sensitive nature within and outside of the Enterprise context, in line with their assigned Security Marking.
26. ICT devices and/or media shall be disposed of using methods commensurate with their security marking and in accordance with relevant legislation⁴.
- (Refer to Implementation Guidelines below: b)*
27. Electronic and physical security controls shall be implemented at the appropriate levels (not necessarily at all available levels), depending on the classification of the data being protected. Individuals shall be allowed access to the data depending on their need to know and security clearance.
28. Individuals or organisations entrusted with the possession and/or use of Government data or equipment shall ensure that the relevant physical and logical controls are in place to prevent:
- Unauthorised access to the data
 - Loss of confidentiality, integrity and availability of the data.
29. Where technically possible and not disruptive to the business, security controls of a workstation or mobile device shall be activated.
- (Refer to Implementation Guidelines below: c, d)*
30. When an ICT device having the potential to access Government data has been lost or stolen, its user shall immediately inform the Data Owner and the Agent.
31. Classified data shall be safeguarded from unauthorised access even when left unattended:
- Desks and other work areas shall be kept clear of data with a security marking of Restricted or higher when left unattended.
 - Screens shall be kept clear of data with a security marking of Restricted or higher when open for public view or left unattended.
 - Any documents containing data with a security marking of Restricted or higher shall be removed from printers and fax machines immediately.
32. Assets located within premises that are not managed by the Agent shall have security controls that take into consideration of the risks of such assets not being hosted in premises managed by the Agent.
33. A trusted device that is not authenticated to a Trusted Identity Provider or to Government Corporate Infrastructure, for a predetermined period of time, shall be removed from the Agent's corporate authentication domain following expiry of such time
- (Refer to Implementation Guideline below: e)*

Implementation Guidelines

For ICT Devices managed by the Agent:

- a. Drive encryption shall be enabled on devices subjected to high travel requirements and that contain sensitive data.
- b. Storage media shall be subjected to wiping, degaussing or destruction, as appropriate.

⁴ L.N. 63 of 2007 Environment Protection Act (CAP. 435) – Waste Management (Electrical and Electronic Equipment) Regulations, 2007

- c. Equipment shall be locked, logged off or switched off when left unattended.
- d. A device shall be automatically locked using a password-protected screen saver after 15 minutes of inactivity.

For systems that are hosted or connect to the Government Corporate Infrastructure:

- e. Removal from the Agent's corporate authentication domain shall occur following 180 days of no authentication.

Asset Management

34. An Asset shall have an identified owner.
35. An Asset shall be utilised under the service parameters through which it was made available to the user.
36. An Asset shall form part of an inventory of assets that shall be kept accurate, up to date and consistent and aligned to other inventories, as applicable, by the respective Government organisation owning it.
37. Upon end of employment, agreement or any other form of engagement, the user shall transfer all relevant data to a corporately governed and managed repository and securely erase it from any other form of storage.
38. Upon end of employment, agreement or any other form of engagement, all Government assets shall be returned within a contractually established period.
39. Any Government identification markings on ICT devices and/or media that the Data Owner shall no longer be responsible for shall be removed.

Access Control

40. The Data Owner shall determine any screening that may be required for any individual or organisation that may access Systems and/or data. Security screening shall be commensurate with the security marking of the data to be accessed.
41. The Data Owner shall authorise the access to be given to an Individual to perform their duties, or to a System to execute its expected function. This access shall be granted according to the least privilege principle.
42. A workstation user is not authorised to grant access to resources on a workstation, other than:
 - for the User to avail of services rendered by the Agent, such as remote support
 - in the case of a locally attached device which does not function as a data store, such as a printer. Such a device shall, however, only be shared with named Users and named workstations.
43. A locally attached device which functions as a data store, such as a pen drive or external hard disc, may only be shared if:
 - it is used solely for work purposes
 - it is scanned by the workstation's endpoint security software
 - Government data stored on the device has security controls that are commensurate with the data's classification⁵.

⁵ Refer to Appendix 1.

44. The Data Owner shall ensure that artefacts of system development are secured from unauthorised access that may impair their intended functionality, their integrity, or infringe the confidentiality of related intellectual property.
45. The Data Owner shall ensure that access rights assigned to an individual shall be reviewed on a regular basis and according to the individual's need to know. Upon expiry, termination or dismissal/removal of employment, contractual agreement or assignment, or long absence from employment, access to the relevant Accounts and associated services, shall be revoked immediately, unless the Data Owner authorises otherwise. The Data Owner shall ensure that reviews of access rights are supported by evidence to demonstrate that they are in line with the least privilege principle based on job function.
- (Refer to Implementation Guidelines below: a)*
46. The Data Owner shall ensure that the process for granting, changing or revoking access rights is implemented and maintained.
- (Refer to Implementation Guidelines below: b)*
47. All systems shall make use of federated authentication mechanisms with trusted identity providers.
48. Access rights may be revoked by the service provider should abnormal behaviour be identified, and the Data Owner shall be advised accordingly. Any re-assignment of access rights shall require authorisation from the Data Owner.
- (Refer to Implementation Guidelines below: c)*
49. A device may be disconnected from the Government Corporate Infrastructure by the service provider should abnormal behaviour of the device be identified, and the Data Owner shall be advised accordingly.
- (Refer to Implementation Guidelines below: d)*
50. An interactive account and associated services shall, where technically feasible, be disabled and/or deleted after a predetermined period of inactivity, unless the Data Owner provides timely justification in writing.
- (Refer to Implementation Guidelines below: e)*

Implementation Guidelines

For Systems managed by the Agent:

- a. The review of access rights shall be carried out at least every 6 months.
- b. The process for granting, changing or revoking access rights shall be the Request for Service (RFS).

For Systems that are hosted on or connect to the Government Corporate Infrastructure:

- c. Revocation of access rights may be carried out by the Agent. Any re-assignment of access rights shall require authorisation from the Agent.
- d. Disconnection may be carried out by the Agent. Any reconnection of the device shall require authorisation from the Agent.
- e. An interactive account used to authenticate with the Agent's corporate authentication service as well as the following associated services and their contents:
 - Mailbox
 - Home folder

- File-hosting service that is corporately approved by the Agent
- Office suite subscription that is corporately approved by the Agent

shall be disabled after 210 days of inactivity following the last password change and **deleted after 2 years of inactivity** following the last password change, unless timely justification in writing is provided.

Account Management

51. An interactive account shall be uniquely named in a manner suitable to enable individual traceability in security audits.
52. Where technically feasible, a generic interactive account shall not be used.
53. A Personalised (named) interactive account shall only be assigned to the individual for whom it is intended. It shall not be transferred to any other party.
54. Requests for personalised (named) interactive accounts assigned to a solution provider or service provider, as well as the resulting accounts created, shall be clearly indicated as such.
55. A personalised (named) interactive account created on the Agent's authentication service shall be provided either one of the following attributes:
 - a valid national identification number, or
 - a valid passport number, or
 - a valid national insurance number, or
 - a valid driving licence number.
56. A non-interactive account shall be Generic and shall not include or bear any resemblance to any Individual login Account name.
57. A non-interactive account shall have an identified owner.
58. A non-interactive account shall not be used interactively.
59. An account with elevated privileges shall be utilised only when the use of an account with lower privileges will not allow a task to be executed.
60. A solution provider or service provider shall be assigned different accounts for each of their employees or contractors.
61. An account shall be assigned to only one Account Holder and shall not be reused by or be reallocated to another Account Holder.
62. Individuals having access to the same stored data shall each have a distinct account for identification, authentication and authorisation purposes.
63. The access rights of any Account shall only apply to its intended System(s) or service(s).
64. It is recommended that for privileged interactive accounts:
 - two-factor authentication or
 - a password stored in an enterprise password vault (preferably using a one-time password mechanism)shall be considered.

Passwords⁶

65. A password shall:
1. be strong, i.e., not null and of adequate length and complexity
 2. not be easily guessed or deduced, or consist of dictionary words
 3. not be identifiable to the context in which it is being applied ⁷
 4. not have repeated or sequential characters, or be pattern-based ⁸
 5. not include three or more consecutive letters from the account holder's name or access credentials
 6. not include common names of people or places
 7. never be displayed or divulged
 8. not be written down or printed
 9. not be stored or transmitted electronically in an unciphered format
 10. only be stored using corporately approved password managers.
- (Refer to Implementation Guidelines below: a, b, c, d)*
66. An individual shall only access and/or make use of a password that he/she is authorised to use.
67. The Data Owner shall identify those passwords that are important for business continuity and disaster recovery purposes. These passwords shall be stored on corporately governed and managed password managers.
68. No default password shall be used.
69. An individual shall, on first use, change a new password that is assigned to him/her.
70. Different passwords shall be used for each different account used by the same individual.
71. Notification prior to expiry of a password shall be given, except for One-Time passwords (OTP).
72. A password change shall not require the intervention of a Solution Provider.
73. A password used for non-work-related purposes shall not be used for accounts accessing Government data.
74. If there is reason to believe that a password has been compromised, the individual identifying such compromise shall inform the Data Owner and the Agent for appropriate action to be taken.

Implementation Guidelines

For Systems that are hosted on or connect to the Government Corporate Infrastructure, Passwords shall have the following attributes:

⁶ These do not include passwords for accounts in use by citizens when consuming public services.

⁷ Such as the name of the service, username, or related derivatives

⁸ For example - keyboard pattern QWERTY

a.Length	<p>For <u>interactive accounts</u> with elevated privileges and <u>non-interactive accounts</u>: minimum of 15 characters.</p> <p>For all other accounts: minimum of 8 characters.</p>
b.Structure	<p>Shall contain at least 3 of the following:</p> <ul style="list-style-type: none">• 1 upper case character• 1 lower case character• 1 number• 1 special character
c.Lifetime	<p>A Password for <u>non-interactive accounts</u> may be set not to expire as long as the <u>System</u> or service makes available the facility to change this password.</p> <p>Passwords for all other <u>non-interactive accounts</u> and all <u>interactive accounts</u> shall be changed every 180 days.</p>
d.Retention of its history	<p>When resetting passwords, the new password shall not be the same as at least the last 2 passwords used.</p>

Protection of Production Data

75. A Production Server shall only be used for production purposes.
76. The use of production data for testing purposes shall be **avoided**. Simulated data providing for testing of all modules/functionalities, including but not limited to data validation, should be created.
77. Where there is no practical alternative to using production data for testing purposes, the data shall be sanitised by removing personal references or by modifying the data to the extent that it is rendered as *Unclassified*.
78. In cases, where the use of exact copies of production data is absolutely required for testing purposes, the applicable environment shall have security controls commensurate with its security marking.
79. Where production data is to be used outside of the production context, authorisation shall be sought in writing from the Data Owner concerned (in consultation with the relevant Data Protection Officer), giving the reasons why production data is absolutely necessary. Such a request shall specify the terms and conditions, including the purposes, related to the use of production data. Without such authorisation, no production data may be used. The Data Owner shall keep a record of such authorisation for audit trail purposes.
80. The role authorized to use such production data shall ensure that the data is erased, following its use as authorised by the Data Owner, and shall inform the Data Owner accordingly in writing. The Data Owner shall keep a record of such communication for audit trail purposes.
81. Backups of production data are considered to be instances of production data. Use of backups of production data shall not be allowed outside the period of authorized use.

82. Movement or disposal of production data shall be commensurate with its security marking.

Cryptographic Controls

83. A cryptographic key shall be protected against disclosure, modification, loss and destruction.
84. Digital Certificates and cryptographic keys used for encryption residing locally on an ICT device shall be backed up and secured by the Individual responsible for the ICT device, on a location which is external to the ICT device.
85. The use of a Digital Certificate shall abide by the terms as issued by its respective Cryptographic service provider.
86. A Digital Certificate may be revoked by authorities of the respective Government organisation issuing it.
87. Respective authorities of a Government organisation may, for investigation purposes, have/be provided access to the cryptographic key for any encrypted Government classified data.
88. Data in storage, data in use and data in transit shall be protected through the implementation of secure versions of protocols, commensurate with the data's security marking.

Where this cannot be achieved, the Data Owner shall seek other measures commensurate with the security marking of the data.

Operational Procedures and Responsibilities

89. Operating procedures, to ensure the correct and secure operation of solutions, shall be documented, maintained and made available to all individuals who need them.
90. The Solution Provider may be requested to provide a report listing the resources outside the hosting environment that are being accessed by an ICT solution and the tools being used for such access.
- (Refer to Implementation Guidelines below)*
91. Changes to Solutions shall be carried out in a controlled manner. A record of such changes shall be maintained.
92. The Data Owner, assisted by the Service/Solution provider, shall ensure that any changes made to the Service/Solution, directly correspond to the registered change request, in line with related Service Level Agreements.
93. System usage shall be regularly monitored and tuned and projections shall be made of future capacity requirements to ensure the required System performance.
94. Government organisations shall ensure that their respective operational procedures cover the monitoring of the performance of backups of data for which they are responsible and the address of any failures which may hinder the completeness of such backups, in line with the requirements of this Policy.

Implementation Guidelines

For Systems that are hosted on or connect to the Government Corporate Infrastructure, a report listing the resources outside the hosting environment that are being accessed by an ICT solution and the tools being used for such access may be requested by the Agent.

Protection from Malware

95. Devices used for interaction with Government data shall, for the duration of such services, have the relevant security controls (such as, but not limited to, anti-virus protection) applied.

(Refer to Implementation Guidelines below: a)

96. The Data Owner shall ensure that Security Controls are implemented for a Solution that is processing Government data to remain free of malware. Such security controls include endpoint security solutions that are provided by the Agent or that are in line with its recommendations.

97. Removable media containing data that has a continuing value to the Government shall be scanned using corporately approved end-point security software.

98. It is every individual's responsibility to ensure that any software is only sourced from reputable, reliable and trustworthy sources and scanned for malware.

E-mail and Internet

99. A personal⁹ e-mail address shall be assigned to only one Account Holder and, upon the Account Holder's expiry, termination, retirement, resignation or dismissal/removal of employment, contractual agreement or assignment, it shall not be reused by, or reallocated to another Account Holder.

100. A suspicious e-mail received from a **known** source should not be opened by the Account Holder before the Account Holder verifies it with the sender.

101. An e-mail from a **suspicious** or **untrustworthy** source shall not be opened. At the recipient's discretion, such an e-mail may be forwarded as an attachment to the Agent's Security Operations Centre (securityoperations.mita@gov.mt) for further investigation. The Account Holder shall subsequently delete the e-mail from their mailbox.

102. E-mail messages that are suspected by the Agent to contain potentially malicious Content and which may therefore constitute a security threat, may be quarantined by the Agent for security reasons without prior notice.

103. Spam originating from Public Administration e-mail domains shall be brought to the attention of the Agent's Security Operations Centre (securityoperations.mita@gov.mt) for investigation and subsequently deleted without forwarding to other Account Holders.

104. Individuals downloading software or files onto any device shall check the software or files for potential malware.

105. Files from unknown or suspicious sources shall never be downloaded on any device that may connect to a Government network.

106. If an account holder is aware of unintentionally contributing to malware (e.g. by submitting credentials to a malicious third party), they shall report it to the Agent's Security Operations Centre (securityoperations.mita@gov.mt) as soon as possible.

Implementation Guidelines

The Agent shall implement and maintain a standard configuration for endpoint security controls **on all the devices that it manages**.

⁹ Address of the Government non-generic email account assigned to an Account Holder for use within Public Administration.

Technical Vulnerability Management

107. Measures shall be implemented to detect and manage technical vulnerabilities in Systems in order to reduce risk from exploitation of technical vulnerabilities. This shall include the review of any default “out-of-the-box” configurations.
108. Intelligence circumventing any security and/or application controls shall not be installed.

Connecting to MAGNET

109. Connection of a trusted network to an untrusted network shall be carried out via adapters¹⁰.
110. The connection of any network to the MAGNET shall be discussed with and shall be subject to approval or otherwise by the Agent.
111. A trusted device or network may be provided with access to relevant *principal* ICT services on MAGNET on a need basis. In the case of remote working, such access through the trusted device shall be provided using a VPN client as approved by the Agent¹¹.
112. An untrusted device or network may be given access to a relevant *controlled subset* of ICT services on MAGNET on an exceptional basis, via adapters and as agreed with and approved by the Agent.
- If alternative protocols are required, these shall be subject to approval by the Agent.
113. Contractors may only be connected to the MAGNET via a logically segregated network, based on the contractor’s level of security clearance and in line with their contractual obligations.
114. The following precautionary measures shall be carried out *before* connecting any device to the MAGNET:
- Latest patches and updates must be installed
 - Anti-virus software shall be installed and up to date.
 - Device shall be free from malware
 - The operating system firewall should be enabled.
 - Ensure that none of the software categories listed in the **Acceptable Use** section are installed.
115. Transmission of data to/from any network connected to the MAGNET shall adopt mutual authentication of end-points and encryption to the appropriate level in relation to the classification¹² of data being transferred.

¹⁰ **Adapter:** A **technical** artefact that allows the interaction between two distinct systems, using standard and secure **protocols, specifically:**

- DNS
- HTTP(S)
- FTP(S)
- SSH
- RDP

¹¹ The Agent’s Security and Governance function

¹² Classification in accordance with the guidelines set out in the Cabinet Office’s Manual of Procedures for the Handling of Classified Information in the Malta Public Service.

Servers

Rationale

It is an ICT Device's use, particularly the type of user interaction, that classifies it as a server. Whilst in its more common role an ICT device that is normally used as a client is not typically regarded as a server, when the same is employed for back office production services and is mostly used in a non-interactive fashion, it simultaneously adopts the role of a server.

This section does not yet cater for server environments hosted on the cloud.

116. Appropriate facility entry controls shall be used to limit and monitor physical access to servers.
117. A Server shall not be taken outside of its principal area of activity without prior authorisation by the respective owners. A Server that is taken outside of its principal area of activity shall have security controls that are commensurate with its risks of operating outside such an area of activity.
118. A Server shall be accompanied by a maintenance agreement.
119. Features such as services, protocols, web servers and other functionalities that are either not required for business operations or which may pose a security risk shall be disabled or reconfigured so as to minimize the associated risk.
120. A Server shall have the relevant security controls enabled and updated at all times.
121. Inactive sessions shall be shut down after a defined period of inactivity.
122. It shall be ensured that, prior to server and/or server media disposal, any sensitive data and software has been securely removed, using a method commensurate with its security classification.
123. Inbound traffic towards servers shall be restricted to the ports required for the server to carry out its intended function/s in accordance with defined business requirements.
124. Inbound traffic towards servers shall only be allowed from those sources that either require access to the services offered by applications or services hosted on the server or are used by individuals authorised to carry out privileged tasks on the server.
125. Access to the Internet from servers shall not be allowed unless required for the server's intended operation, in which case approval is required by the Data Owner. Patch management solutions should be considered to avoid direct connectivity to the internet as much as possible.
126. Non-console administrative access shall be encrypted.
127. For servers handling data classified as *Restricted* or above, outbound traffic shall be limited to:
 - responses to incoming connections to the server
 - connections required in support of the services offered by the server
 - outgoing connections required for the continued proper functioning of the server
128. Configuration standards for server operating system hardening shall be documented.

Backup and Restoration

129. All production data shall be backed up according to an established backup schedule.

The backup schedule shall reflect the:

- Business requirements
- Security requirements and classification
- Business continuity requirements
- Technical and financial considerations

Any other requirements need to be brought to the attention of the service/solution provider by the Data Owner.

130. For disaster recovery purposes, backup arrangements for critical services shall cover all related system information, applications and data necessary.

131. It is every individual's responsibility to ensure that all data that has a continuing value to the Government is backed up on corporately governed and managed repositories. Keys for encrypted data shall be made available to authorised personnel as and when required to ensure business continuity.

132. The Data Owner shall ensure the integrity and availability of backups for data for which they are responsible. The Agent shall perform backups and restores as requested by the Data Owner. The integrity and availability of backups shall be ensured for their lifetime.

133. Requests for data restoration shall be recorded and shall require authorisation from the Data Owner. Data restoration records shall include:

1. Requester name
2. Name of Data Owner authorising the request,
3. Data description
4. Operation date
5. Outcome

134. Backups of production data shall be subject to the same security controls as the production data.

135. The storage of Government data, carrying a security marking of *Restricted* or above, on removable storage devices may only be considered if such data is secured commensurate with its security marking.

136. Non-work-related data shall not be stored on corporately governed and managed repositories.

Clock Synchronisation

137. The clocks for all relevant information processing systems within a Government organisation shall be synchronised to a reference time source in the following order of precedence:

1. Through the locally competent authority for such a service
2. Through a European Union (EU) competent authority for such a service
3. Through any open access time source as listed on the NIST Internet Time Service (ITS).

Audit Data

138. Wherever audit data identified by the Data Owner is being generated, this shall be accessed and/or disclosed, unaltered and in native format as authorised by the Data Owner or as requested by competent authorities for investigation purposes as established by law.
139. As a minimum, audit data records shall include:
1. Timestamp
 2. Source, Context and/or Identity
 3. Operation
 4. Outcome
140. Audit data shall not be tampered with or be subject to unauthorised reading.
141. Access to and disclosure of audit data shall only be authorised by the Data Owner.
142. Audit logging facilities may only be deactivated if authorised by the Data Owner.
143. Audit logging facilities interacting with Systems managed by the Agent shall be segregated and restrictions applied to their access and use in order to reduce risk of unauthorised or unintentional disclosure or modification of the audit data.
144. Audit data shall have the same security marking as that of the data being processed by the Solution. As a minimum, be assigned a Security Marking of *Unclassified*.
145. Backups of audit data are considered to be instances of audit data. Government organisations shall determine the retention period for audit data applicable from the instant at which the data is generated by the original source. Following this period, the audit data shall be considered as expired and shall be overwritten, destroyed or deleted. If requested otherwise in writing during this retention period by the Data Owner or by the competent authorities for investigation purposes as established by law, the data shall be retained for the period requested.
146. Audit data may be stored either in the Agent's security information and event management solution, subject to the latter's approval, or in an appropriate corporately governed and managed logging solution. Access to the Agent's security information and event management solution shall be limited to its Security and Governance function.

System Acquisition, Development and Maintenance

147. Information security related requirements shall be included along with requirements for development or acquisition of new systems or for enhancements of existing systems.
148. A System shall carry out validation checks upon data input, output and processing.
149. Implemented security controls shall be commensurate with the highest level of security marking of the data processed by a system.
150. Rules for the development of systems shall be established and applied.

Information Security incident management

151. The Data Owner shall ensure that event logs recording user activities, faults and information security events are produced, kept and regularly reviewed.

152. Where technically possible, event logs shall record whether or not personally Identifiable Information has been changed as a result of an event and who performed the change.

153. Information security events, information security incidents, security weaknesses, observed or suspected information security abnormal activities impacting Government data shall be reported to the Data Owner.

(Refer to Implementation Guidelines below: a)

154. Upon becoming aware of any information security event, information security incident and/or security weakness related to an ICT solution managed by a Solution Provider, the Solution Provider shall immediately take all necessary steps to assess, contain and rectify it, as agreed with the Data Owner.

(Refer to Implementation Guidelines below: b)

Implementation Guidelines

For Systems that are hosted on or connect to the Government Corporate Infrastructure:

- a. These shall also be reported to the Agent's Security Operations Centre (securityoperations.mita@gov.mt). Following an assessment, the latter may escalate an information security event to an information security incident.
- b. The Agent may require particular steps to be taken.

Business Continuity Management

155. The Data Owner, assisted by the Service/Solution provider, shall plan, implement, test and review business continuity arrangements related to any critical activities supporting the delivery of Government ICT services. Solutions shall be implemented with redundancy sufficient to reflect availability requirements.

156. Where possible, generic e-mail accounts shall be used instead of personalised (named) accounts, for business continuity purposes.

Information Security Reviews

157. The approach to managing information security and its implementation shall be reviewed independently at planned regular intervals or when significant changes occur, to ensure conformance to and the effectiveness of related applicable policies, standards and measures.

158. When operating platforms are changed, business critical applications shall be reviewed and tested to ensure that there is no adverse impact on organizational operations or security.

159. Security assessments shall be carried out in order to assess any related risks.

(Refer to Implementation Guidelines below)

Implementation Guidelines

For Systems that are hosted on or connect to the Government Corporate Infrastructure, security assessments shall be carried out by the Agent's Security

Engineering function (securityengineering.mita@gov.mt) and/or Security Governance function (securitygovernance.mita@gov.mt).

Intellectual Property Rights

160. Any artefact created:

- as a result of employment or contractual obligations with a Government organisation, or
- following instructions in writing by a Government organisation

shall be owned by the Government organisation, unless agreed otherwise in writing by the Government organisation and the author of the work.

161. The author of the intellectual property shall seek authorisation in writing from the Government organisation for its use, giving detailed reasons for such a request. It shall be the sole discretion of the Government organisation to accept or refuse the request.

162. Authors of Intellectual Property that constitutes research data shall, however, have a non-exclusive license to use such data for educational, research and scholarly purposes without making profit. Such use shall be limited to the term of the contractual relationship between the Government organisation and the author.

163. Third Party Intellectual Property Rights that are licensed to a Government organisation shall be used in accordance with the applicable license terms and conditions.

Acceptable Use

164. Installation of software that is specifically required by the business (line of business software) and was not originally installed on the workstation shall require the authorisation of the respective CIO.

165. Different versions of a software product, as well as software products that are bundled inside the same download package, may introduce their own specific security vulnerabilities. Therefore, they are to be considered as separate software products and require separate authorisation.

166. The CIO shall ensure that the software is compatible with the workstation's standard configuration controls in place.

167. The user of the software product shall ensure adherence to its associated terms of the license.

168. The Agent may audit and monitor any impact stemming directly or otherwise from such software installed.

169. All software installed on an ICT device shall be patched with the latest updates, in line with a documented patch management procedure. Line of business software shall be patched by the user of the workstation upon which this software is installed.

170. The following software categories are not allowed on any device that connects to the MAGNET:

- Packet sniffers
- Password/key cracking software
- Port/vulnerability scanners
- Hacking tools

- Packet crafting tools
- Key loggers
- Key generators
- Credit Card number generators

These software types may **only** be used for **investigation** purposes by bodies/personnel authorised by the Agent.

The following are **not allowed** for corporately governed and managed devices (unless approved by the Agent), but **allowed** for other devices (such as those used by suppliers/contractors):

- E-mail clients
- VPN clients
- Tethering software
- Proxies
- DNSs

171. VPN services on devices that are corporately governed and managed shall be subject to approval or otherwise by the Agent should they be required within the enterprise context.

172. VPN services, other than those provided by the Agent, shall not be allowed to run simultaneously on trusted and/or untrusted devices whilst accessing Government ICT services. The same applies to tethering.

Account management for specific work life instances

173. When an Account Holder moves to a different Government Ministry or Entity, their Account, email address and associated services shall be deleted-unless the Data Owner of the Ministry or Entity from which the Account Holder is moving approves the Account Holder's retention of the original Account, e-mail address and/or associated services.

174. An Account Holder returning to a Ministry or Entity after-movement to another Ministry or Entity, expiry of employment or resignation, shall be treated as a new employee and shall be assigned a new Account, e-mail address and associated services, unless the Data Owner of the Ministry or Entity to which the Account Holder is returning, approves the Account Holder's reassignment of their original Account, e-mail address and a copy of the backup of their associated services, if it still exists.

175. When an Account Holder moves to a different department or function within the same Government Ministry or Entity or is seconded to another Government Ministry or Entity, their Account, email address and associated services may be retained only if the Data Owner of the department or function from which the Account Holder is moving approves this.

176. In the case of long period of absence from employment, the Account Holder shall retain their Account, e-mail address and access to their associated services, to ensure a channel through which official communication may be received by the Account Holder¹³. For business continuity purposes, it is the responsibility of the Account Holder to inform accordingly through an 'out of

¹³ In line with *Manual on Special Leaves or the Manual on Work-Life Balance Measures*
<https://publicservice.gov.mt/en/people/Pages/PeopleSupportandWellbeing/absences.aspx>

office' reply. The Data Owner shall also decide whether access to other Systems is to be allowed or revoked.

177. An Account Holder's use of their Account, e-mail address and/or access to their associated services may be suspended or terminated for several reasons upon authorisation by the Data Owner.

Human Resource Security

178. Requirements for confidentiality or non-disclosure agreements reflecting a Government organisation's needs for the protection of data and operational details shall be identified, documented and reviewed at planned, regular intervals.

Appendix 1: Security Marking List¹⁴

Security Marking	Description ¹⁵	Preparation and handling	Access	Copying and Storage	Exchange	Archive or disposal
Top Secret	Data, information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of Malta, the EU, NATO or one or more of their Member States.					
						Applicable procedures by the appropriate authority ¹⁶ .
Secret	Data, information and material the unauthorised disclosure of which could seriously harm the essential interests of Malta, the EU/NATO or one or more of their Member States.					
Confidential	Data, information and material the unauthorised disclosure of which could be detrimental to the essential interests of Malta, the EU, NATO or one or	Clear <u>Security Marking</u> and date are required. Data shall be encrypted.	On a right to know and need to know basis. Only named individuals/roles shall have access to the data.	On a right to know and need to know basis. Data shall be encrypted.	On a right to know and need to know basis. Data shall be encrypted.	In line with the requirements of the National Archives Act CAP 477. Method: <u>Purging</u> .

¹⁴ Does **not** apply to physical representations of Government data.

¹⁵ Security Marking descriptions are the same as those in the Manual of Procedures for the Handling of Classified Information in the Malta Public Service.

¹⁶ Manual of Procedures for the Handling of Classified Information in the Malta Public Service

Security Marking	Description ¹⁵	Preparation and handling	Access	Copying and Storage	Exchange	Archive or disposal
	<p>more of their Member States.</p> <p>It includes:</p> <ul style="list-style-type: none"> - Data for which there is a legislative, contractual or regulatory obligation on <u>Government</u> or its employees to protect it - Data which, if subject to unauthorised disclosure, modification or destruction, could give rise to a security breach; such a security breach could happen with minimal effort due to lack of adequate compensating controls in place. <p>Examples of the significant impact which may result if confidential data is not protected include:</p>	<p><u>Security marking</u> shall be made evident, without the need to decrypt the data.</p>	<p>If data is accessed from an ICT device not owned by the data's intended recipient, the data shall be removed.</p>		<p>Explicit authorisation shall be required for data to be exchanged both within and outside of the <u>Enterprise context</u>.</p> <p>Should the data originate outside of the <u>Enterprise context</u>, authorisation shall be required for its exchange within the <u>Enterprise context</u>.</p> <p>Transmission of encrypted data and its related encryption key shall be conducted through separate transmission channels.</p>	

Security Marking	Description ¹⁵	Preparation and handling	Access	Copying and Storage	Exchange	Archive or disposal
	<ul style="list-style-type: none"> - Breach of law - Financial impact - Security breach/incident 					
Restricted	<p>Data, information and material the unauthorised disclosure of which could be disadvantageous to the interests of Malta, the EU, NATO or one or more of its Member States.</p> <p>Data that is restricted requires named individuals/roles to have access to it. The disclosure of such data may result in undesirable consequences such as:</p> <ul style="list-style-type: none"> - Unfair advantage to unauthorised recipients - Damage to the reputation of <u>Government</u> <p>Offline email data files shall, as a minimum, be assigned this marking.</p>	<p>Clear <u>Security Marking</u> and date are required.</p> <p>Encryption is recommended.</p>	<p>On a right to know and need to know basis.</p> <p>Only named individuals/roles shall have access to it.</p>	<p>On a right to know and need to know basis.</p> <p>Encryption is recommended.</p> <p>Data that is persisted on portable media or mobile devices shall be encrypted or password-protected as a minimum.</p>	<p>On a right to know and need to know basis.</p> <p>Encryption is recommended.</p>	<p>In line with the requirements of the National Archives Act CAP 477.</p> <p>Method: <u>Purging.</u></p>

Security Marking	Description ¹⁵	Preparation and handling	Access	Copying and Storage	Exchange	Archive or disposal
Unclassified	Data that does not fall under any of the above <u>security markings</u> .	Clear <u>Security Marking</u> and date are recommended.	On a right to know and need to know basis.	On a right to know and need to know basis.	On a right to know and need to know basis.	In line with the requirements of the National Archives Act CAP 477 . Method: <u>Erasure</u> .

Deviations from GMICT Policy

Instances where it may not be technically possible or cost-effective to comply with a particular GMICT Policy requirement shall be reported as risks at <https://rrs.gov.mt> to be assessed.

Breaches of GMICT Policy shall be brought to the attention of the respective CIO office in order to determine appropriate corrective action and potential control improvements involving relevant stakeholders, as appropriate.

Issuing Authority

This document has been issued with the authority of the **Principal Permanent Secretary**.

Contact Information

Government ICT Policies may be found at <https://ictpolicies.gov.mt>.

Any suggestions, queries or requests for clarification regarding Government ICT Policies may be forwarded to ictpolicies@gov.mt.