GOVERNMENT DATA SECURITY POLICIES

This document contains general information for the public only. It is not intended to be relied upon as a comprehensive or definitive guide on each agency's policies and practices. The data security measures implemented by each agency will differ depending on various factors such as the sensitivity of the data and the agency's assessment of data security risks. The Government may update the policies set out in this document without publishing such updates to the public.

SMART NATION & DIGITAL GOVERNMENT OFFICE

The Government takes its responsibility as a custodian of data very seriously.

Since 2001, the Government's data security policies have been set out in the Government Instruction Manual (IM) on Infocomm Technology and Smart Systems (ICT&SS) Management. In 2019, the Public Sector Data Security Review Committee recommended additional technical and process measures to protect data and prevent data compromise. The recommended measures have since been incorporated into the IM on ICT&SS Management.

This document sets out the key policies in the IM on ICT&SS Management that govern how data security is managed by agencies. The policies prescribe data security requirements, including technical and process measures, to safeguard data against security threats.

The technical and process measures described in this document are implemented using a risk-based approach. Agencies should select the measures based on the data security risk level, after taking into account their operating contexts. For example, the recommended measure "Hashing-with-Salt" irreversibly changes a data field in order to prevent an attacker from accessing the original value of the data field even when the data is extracted from the system. It would be suitable for use in analytics systems where only de-identified data is required but not appropriate for use in operational systems which require identifiable data for service delivery.

Note: This document contains general information for the public only. It is not intended to be relied upon as a comprehensive or definitive guide on each agency's policies and practices. The data security measures implemented by each agency will differ depending on various factors such as the sensitivity of the data and the agency's assessment of data security risks. The Government may update the policies set out in this document without publishing such updates to the public.

Section 1: Data Security Risk Management

01 To ensure adequate and effective data security risk management, Agencies should perform data security risk assessments for their datasets, as part of the Government ICT Risk Management Methodology.

This will enable Agencies to identify data security risks, evaluate the risks, implement measures to mitigate the risks, assess the effectiveness of the implemented measures and manage the risks within limits acceptable to the Agency.

02 Agencies should use the Data Security Risk Assessment Methodology, which is part of the Government ICT Risk Management Methodology, to conduct data security risk assessments for their datasets.

03 Agencies should conduct a data security risk assessment:

a) When acquiring a new dataset;

b) Developing a new ICT system that contains personal or entity data; or

c) When existing data which has not been risk assessed is first used.

04 Agencies should review the data security risk assessments:

a) According to the frequency stated in the Government Risk Management Policy; or

b) When there are changes to the data security risk factors.

Section 2: Technical and process measures to protect data and prevent data compromises

05 Agencies should implement the appropriate technical and process measures to protect data against data security threats and prevent compromises of the confidentiality and integrity of the data.

Agencies should adopt a risk-based approach when implementing the technical and process measures. Technical measures are only effective when the complementary process measures are implemented too (See Annex A).

The data security technical and process measures are to be implemented on top of any cybersecurity measures in place.

Data should be protected according to the risk level determined through a data security risk assessment. Agencies should ensure that data is adequately protected while minimising the impact to operations, resources and costs.

06 Agencies should adopt the following strategies when implementing the technical measures and process measures to safeguard data:

a) Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads;

b) Enhance the logging and monitoring of data transactions to detect risky or suspicious activity; and

c) Protect data in a manner that will render the data unusable even if extracted.

Section 3: Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads

07 Agencies should minimise the surface area of attack, i.e. the different points through which a threat actor can compromise data security, by using the following 3 approaches:

a) Collect, retain, and store data only where necessary;

b) Minimise the download of data to endpoint devices; and

c) Access and use data only for the task at hand.

Section 3.1: Collect, retain, and store data where necessary

Collect datasets only where necessary

08 Agencies should minimise the collection of datasets to only what is necessary for their functions and operations. For each collected dataset, Agencies should identify the specific use of the dataset, and whether the dataset is required to carry out an immediate function or a pre-requisite to carry out a future function (e.g. longitudinal datasets for analytics purposes) or both. Where the dataset includes data on individuals, Agencies should also collect the data in accordance with the Government's personal data protection policies.

Limit retention period of data

09 Agencies should ensure that every dataset collected is stored only for the period that is necessary to fulfil the purposes for which the dataset is collected, subject to any legal or Agencies' archival requirements. Where the dataset includes data on individuals, Agencies should also retain the data in accordance with the Government's personal data protection policies.

10 Agencies should set a retention period for each dataset.

11 Agencies should consider instituting processes to ensure that data is purged from ICT systems and user devices when the retention period for the data is over. Data retained to fulfil archival requirements should be transferred to archival systems.

Section 3.2: Minimise the download of data to endpoint devices

Secured isolated environments for high-risk users

12 To minimise the risk of data exfiltration, Agencies should ensure that users, assessed by Agencies to be high-risk, access sensitive data only in secured isolated environments. Such isolated environments can be secured physically ("Physically Secured Isolated Environment") or virtually ("Virtually Secured Isolated Environment").

13 Agencies should ensure that the high-risk user's access to the data in a physically secured isolated environment (i.e. an ICT system that contains sensitive data and is not connected to any other systems) is monitored at all times and technical measures should be implemented in the ICT system to stop any unauthorised transfer of sensitive data out of the environment.

14 Agencies should ensure that the high-risk user's access to the data in a virtually secured isolated environment (i.e. an environment equipped with ICT infrastructure that stops the exfiltration of data from the ICT system containing the sensitive data) is monitored at all times.

Retrieve only the data required instead of data dumps

15 Agencies should ensure that users request and retrieve only the data required to complete their assigned tasks and that users do not retrieve more data than needed.

16 Agencies should implement processes to ensure that when data is stored in documents or files, a user is given access to only the data fields and data records relevant to the user's needs.

17 Agencies should implement processes to ensure that data stored within databases is accessed by users through data queries as far as practicable.

Access sensitive files on secured platforms

18 To minimise the risk of sensitive data being compromised on user devices, Agencies should ensure that sensitive data can only be accessed through Agencies' or central Whole-of-Government secured platforms, where practicable.

The secured platforms are to have the following features:

a) The necessary ICT and data security measures to protect the data;

b) Access control to the platform; and

c) Logging of access.

19 Where practical, Agencies should utilise the secured central document collaboration platforms for accessing, sharing and editing of documents containing data.

20 Where practical, Agencies should utilise the secured data platforms of the Government Data Architecture to access, share and analyse data.

Section 3.3: Access and use data for task at hand

21 Agencies should implement processes and controls to ensure that:

a) The rights to access data are granted on a need-to-know basis;

b) The rights to access data are regularly reviewed;

c) Users are able to access only data that they have been granted access rights to; and

d) The task at hand falls within the purposes for which the use of data is permitted, before using the data.

Volume limited and time limited data access

22 Agencies should limit the volume of sensitive data in ICT systems that can be accessed by users, and the duration for which users can access the sensitive data. This prevents users from accessing too much sensitive data within the pre-determined period of time.

23 Agencies should set predefined limits for:

a) The volume of sensitive data to be accessed; and

b) The duration of access to sensitive data.

Agencies should restrict data access when the volume or the duration of data accessed exceeds predefined limits. This should be done through:

a) Use of access control features of ICT systems, together with logging and monitoring of data access controls; or

b) Requiring user re-authorisation when the duration or volume of data accessed exceeds the predefined limits.

Automatic Identity and Access Management tools

24 Agencies should implement Automatic Identity and Access Management tools to automate the management of users' identity and access rights. This is to ensure that only authorised people are granted access to the data at any point in time.

Limit and monitor authorised and privileged access to sensitive data in ICT systems

25 Agencies should put in place processes to ensure that access to sensitive data in ICT systems is granted only to authorised users, and privileged access to data is granted only where necessary. Users' access to sensitive data should be regularly reviewed and removed expeditiously when the user's role changes. This is to reduce the risk of unauthorised access to sensitive data.

26 Agencies should ensure an authorised user's access to sensitive data is limited to the sensitive data needed for a stated purpose of use.

27 Agencies should ensure that access to data by users with privileged accounts or users who hold privileged data roles, are limited to the ICT systems, data platforms, and datasets needed to carry out the users' functions.

Section 4: Log and monitor data transactions to detect risky or suspicious activity

28 Agencies should log and monitor data transactions to detect suspicious or risky activities and take action to prevent any potential data compromise.

Agencies should do this by:

a) Maintaining logs and records to pinpoint risky activities, detect suspicious activities, and to assist in response and remediation; and

b) Deploying tools to detect suspicious activity and alert the relevant parties to respond to such activities.

Section 4.1: Maintain logs and records to pinpoint high-risk activities and to assist in response and remediation

Maintain data lineage for data to support data incident management

29 Agencies should keep data lineage records for data. Data lineage records help to identify any unauthorised access, usage or modification of data. Data lineage records support Agencies in managing and responding to data incidents.

The data lineage records should be tracked at the dataset's meta data level but need not be tracked for every change made to the dataset. The data lineage records should cover how the data is used, how it flows between users and systems, and the key changes made to the dataset.

Digital watermarking of file

30 Agencies should implement digital watermarking on files containing data to identify the originator of the files, unless the files:

a) Are system generated; or

b) Cannot be digital watermarked by readily available tools.

31 Agencies should ensure that the digital watermark:

a) Contains information that identifies the originator of the file; and

b) Allows the recipient of file to readily identify the originator of the file by displaying the identifying information or revealing the information when the file is examined with the appropriate digital tool.

Section 4.2: Deploy tools to detect suspicious activity and alert the relevant parties for incident response

Enhanced logging and active monitoring of data access

32 Agencies should log, actively monitor and analyse data access to detect anomalous activities and to support remediation when data incidents occur.

33 Agencies should maintain logs of access to data. The logs should show what data has been accessed, how it has been accessed and who accessed it. In addition, the logs should be protected from accidental or deliberate modification or erasure.

34 Agencies should ensure active monitoring of data access to sensitive data by scanning for signs of data security compromise and actively checking ICT systems and data platforms for compliance with the data security rules.

Email data protection tools

35 Agencies should implement email data protection tools that detect potentially risky data transfers and prompt users for confirmation of such data transfers to prevent any accidental or unauthorised disclosure through email. This clause is not applicable for system generated emails.

Data loss protection (DLP) tools

36 Agencies should implement DLP tools in their endpoint devices, IT networks and other ICT systems containing sensitive data. The DLP tools should monitor the endpoint devices, networks and ICT systems for possible data loss, alert the user to potentially risky user action which might result in data compromise, and detect and prevent any unauthorised data transfers.

37 Agencies should implement DLP tools to cover all possible avenues of data loss from their ICT systems. This includes endpoint devices and network systems.

Agencies are to implement DLP tools that have the following features:

a) Able to read the security and sensitivity classification of a document as determined by the user;

b) Able to alert the user or require user affirmation on authorised but potential risky user action involving data, as determined by the DLP rules;

c) Able to stop the user from executing an action which will result in a violation of the DLP rules; and

d) Able to monitor for violations of the DLP rules.

Section 5: Protect the data directly when it is stored and distributed to render the data unusable even if extracted

38 Agencies should protect the data directly to render the data unusable to an attacker if extracted from ICT systems. This provides an additional layer of defence on top of the other cyber security and data security measures.

The 3 approaches that Agencies may take to protect data in this manner are:

a) Render sensitive data unusable to an attacker, even if exfiltrated from storage;

b) Partially hide the full data. Even if the sensitive data is exfiltrated, the damage would be limited as the attacker would not have access to the full data; and

c) Protect the data during distribution. This reduces the risk of accidental data compromises due to human error when sending emails with sensitive data.

Section 5.1: Render sensitive data unusable to an attacker, even if exfiltrated from storage

39 Agencies may choose one of the following technical measures to protect sensitive data and render the data unusable to an attacker even if exfiltrated from storage:

a) Hashing with salt;

b) Field Level Encryption; or

c) Tokenisation.

Hashing with Salt

40 Agencies should ensure that sensitive values to be protected are combined with a secret value, called the salt, before applying a cryptographic hashing function to generate a hashed value that cannot be reversed with current computing resources.

41 Agencies should consider using "hashing with salt" where the actual values need not be recovered but can be transformed into a unique reference.

For example, hashing with salt is suitable to protect identifiers in data in data analytics use cases where there is no need to identify the entities.

Field Level Encryption

42 Agencies should ensure that sensitive values to be protected are encrypted at the field level.

Within a dataset, only authorised users should be allowed to access and decrypt the values protected by Field Level Encryption. Other users of the dataset that are not authorised to access the protected values, should not be allowed to access and decrypt the protected values.

43 Agencies should consider using Field Level Encryption when the actual values of the sensitive data are frequently required. The encrypted value can be decrypted using the correct decryption key by an authorised user.

For example, field level encryption is suitable for service delivery systems where there is a need to correctly identify an individual in order to deliver a service.

Tokenisation

44 Agencies should ensure that sensitive values to be protected are replaced with token values and that the original values cannot be reasonably recovered from the token values. The mapping between the original values and token values should be kept securely and separated from the tokenised data set.

Manage keys to data protection technical safeguards

45 Agencies should put in place processes to manage keys used in the technical measures to protect data directly. These processes should ensure that the key is well-managed and safeguarded throughout its lifecycle: generation, exchange, storage, usage, replacement, and destruction of keys.

46 In relation to clause 45, the keys that may be managed by Agencies include:

a) Salt value of hashing with salt;

b) Encryption and decryption keys of Field Level Encryption; and

c) Mapping of token value of tokenisation.

47 Agencies should ensure proper separation of roles of the persons using the protected data and the persons managing the keys.

Section 5.2: Partially hide the full data

48 Agencies should hide sensitive data fields by implementing the following technical measure(s) as appropriate:

a) Obfuscation/ masking/ removal of entity attributes; or

b) Dataset partitioning.

Obfuscation/ masking/ removal of entity attributes

49 Agencies should ensure users who do not need to access the exact data values of sensitive data are presented with partially hidden data values that are less sensitive but sufficient for usage and exploitation to complete their assigned tasks.

50 Agencies should consider hiding the true value of the attributes by adding noise, banding the data, or masking portions of the value. Attributes not relevant for data usage should be removed.

Dataset partitioning

51 Agencies should reduce data concentration risk by partitioning sensitive data into smaller datasets. This can be done by segmenting out selected entities, individuals or attributes and applying different access controls to each of the partitions. This reduces the likelihood of compromise of the selected entities, individuals or attributes should the larger dataset be compromised.

52 Agencies should consider partitioning the dataset by either:

a) Physically partitioning the dataset in different storage locations; or

b) Virtually partitioning the datasets in different virtually isolated partitions.

Each dataset partition, physical or virtual, should have different access controls.

Section 5.3: Protect the data during distribution

Password protecting and encrypting files when distributing files through unsecured channels

53 Agencies should ensure that files containing sensitive data are secured with password and encryption when the file is distributed through unsecured channels and where there is possible unauthorised access to the file. Password protecting and encrypting the files ensure that only authorised users are permitted to access the content of the file.

Securely distribute passwords out-of-band

54 Agencies should ensure that encrypted data files and their passwords are securely distributed out-of-band through separate channels. This is to prevent compromise of both the protected data files and passwords during transit due to malicious interception or accidental disclosure. Password hints may be sent in the same channel.

Data file integrity verification

55 Agencies should adopt data file integrity verification measures to ensure the integrity of a file containing sensitive data, when the file is being transferred between users.

56 Agencies should verify the file integrity using cryptographic hash standards.

Distribute files through approved secure channels

57 Agencies should distribute files containing data via proper channels that are safeguarded by required security measures commensurate with the security classification of the data.

58 Agencies should ensure that the distribution channels are encrypted.

Protect sensitive data when distributing via email

59 Agencies should ensure that sensitive data is protected from unintended disclosure when sending via email.

60 Agencies should:

a) Ensure that emails containing sensitive data are addressed to the correct recipients;

b) Use a mailing list for regular mass communication to specific groups; and

c) Send emails via Blind Carbon Copy (BCC) when mass emailing parties outside of the Whole-of-Government.

61 Agencies should ensure users:

a) Password-protect and encrypt files containing sensitive data; and

b) Perform data file integrity verification for files where integrity is critical.

ANNEX A

SMART NATION
&
DIGITAL GOVERNMENT OFFICE

Technical measures and the process measures

Technical Measures	Clause Number
Volume limited and time limited data access	22
Automatic Identity and Access Management tools	24
Log and monitor data transactions to detect high-risk or suspicious activity	28
Digital watermarking of file	30
Email data protection tools	35
Data Loss Protection (DLP) tools	36
Hashing with Salt	40
Field Level Encryption	42
Tokenisation	44
Obfuscation/ masking/ removal of entity attributes	49
Dataset partitioning	51
Password protecting and encrypting files when distributing files through unsecured channels	53
Data file integrity verification	55

Process Measures	Clause number
Collect datasets only where necessary	8
Limit retention period of data	9
Secured isolated environments for high-risk users	12
Retrieve only the data required instead of data dumps	15
Access sensitive files on secured platforms	18
Limit and monitor authorised and privileged access to sensitive data in ICT systems	25
Maintain data lineage for data to support data incident management	29
Manage keys to data protection technical safeguards	45
Securely distribute passwords out-of-band	54
Distribute files through approved secure channels	57
Protect sensitive data when distributing via email	59

Technical measures and the complementary process measures

Technical Measures	**Complementary Process Measures**
Volume limited and time limited data access	Limit retention period of data
Automatic Identity and Access Management tools	Limit and monitor authorised and privileged access to sensitive data in ICT systems
Log and monitor data transactions to detect high-risk or suspicious activity	
Digital watermarking of file	-
Email data protection tools	Protect sensitive data when distributing via email
Data Loss Protection tools	Distribute files through approved secure channels
Hashing with Salt	Manage keys to data protection technical safeguards
Field Level Encryption	
Tokenisation	
Obfuscation/ masking/ removal of entity attributes	-
Dataset partitioning	-
Password protecting and encrypting files when distributing files through unsecured channels	Securely distribute passwords out-of-band
Data file integrity verification	-

Glossary of Terms

Terms	Definition
Agency	Agency refers to Organs of State, Ministries, Departments and Statutory Boards.
Collection	Collection refers to the act of gathering, acquiring, or obtaining data from any source, and whether directly or indirectly by any means.
Business data	Business data refers to data, whether true or not, which are related to an identified or identifiable company or other incorporated or unincorporated body of persons
Data	Data refers to the representation of information that can be used for communications or processing. Broad categories of data are structured and unstructured data.
Dataset	A dataset refers to a collection of data which can exist in digital documents (such as Excel files), be stored in ICT systems (such as in databases) or recorded in hardcopy.
Data query	A data query is a request for specific data fields and data records.
Data Security Risk Assessment Methodology	The Data Security Risk Assessment Methodology guides agencies in the identification, analysis and treatment of data security risks inherent in datasets. As part of the methodology, agencies perform risk assessments to identify data security risks, evaluate the risks, determine the controls to mitigate the risks, assess the effectiveness of the controls implemented and manage the risks within acceptable limits to the agency.
Disclosure	Disclosure refers to making data available to others.
Document	Document refers to information recorded in any form.

Endpoint devices	Endpoint Devices refer to end-user devices designed for individual use (can be used by one or more users), such as personal computers, mobile devices, IP phones used to store, process or access Government data.
Entity	Entity refers to a company or other incorporated or unincorporated body of persons.
Entity data	Entity data refers to any data, whether true or not, which are related to an identified or identifiable entity.
Government ICT Risk Management Methodology	The Government ICT Risk Management Methodology guides agencies in the identification, analysis and treatment of cybersecurity and data security risks inherent in systems. Under the methodology framework, agencies perform risk assessments to identify the ICT risks, such as ICT security and data risks to their systems, assess the consequent risks to the Agency, determine the controls to mitigate the risks, and assess the effectiveness of the controls implemented.
Government Risk Management Policy	The Government Risk Management Policy defines: 1) The Government ICT Risk Management methodology; 2) The standards for managing ICT risks, such as frequencies of audits; and 3) The thresholds for Agencies risk exposures.
ICT system	ICT System refers to a set of interacting, interrelated, or interdependent ICT hardware, software and data created, accessed, stored, processed or transmitted to serve business functions and support business operations.
Individual	Individual refers to a natural person, whether living or deceased.
Personal data	Personal data refers to any data, whether true or not, which are related to an identified or identifiable person.
Privileged access	Privileged access refers to access granted to any user with privileged accounts or holding privileged data roles.

Privileged accounts	Privileged accounts refers to accounts used by personnel for performing network, system, application-wide, agency-wide, or Whole-of-Government-wide administrative/security activities such as the following: • Creating, modifying, or deleting accounts and their privileges; • Creating, modifying, or deleting security tokens; • Setting, modifying, and removing configurations; • Installing or uninstalling software; or • Accessing, creating, modifying, or deleting system-restricted data. Examples of personnel that uses privileged accounts are system administrators, database administrators, and personnel who administrates for the entire application. These personnel use privileged accounts to perform activities such as account management, cryptographic key management, database administration, network administration, and system administration.
Privileged data role	Privileged data roles refer to user roles that are able to access, create, modify, or delete data where the data access has not been personally and explicitly granted but gained by the virtue of the roles' job functions that require access to the data platforms and systems that contain the data. Examples of privileged data roles are data scientists and data engineers who have access to data on data platforms and systems for the purpose of data processing etc. System administrators and database administrators who have access to privileged accounts will also be considered as having privileged data roles.
Security classification	Security Classification refers to classifying information according to the security levels that measure the damage done to national security, or national or Agency interest, in the event of an unauthorised disclosure.
Sensitive	Sensitive refers to data if leaked could give rise to discrimination or other negative impact on a data subject (e.g. the person's insurability, employability, reputation, etc.).
Sensitivity classification	Sensitivity Classification refers to classifying information according to sensitivity levels that measure the damage done to an individual or an organisation, in the event of an unauthorised disclosure.
Use	Use refers to the treatment and handling of data within an agency.
User	Users refers to all Government officers and non-Government personnel who are granted access to Government Resources to perform official work for the Government.