POLICY TITLE:	Data Classification Standard

Overview

This standard defines the classification scheme and outline the expected data handling requirements throughout the lifecycle of data. Recommended disclaimers to be used when storing and transferring data of various classifications will be defined in this document as well.

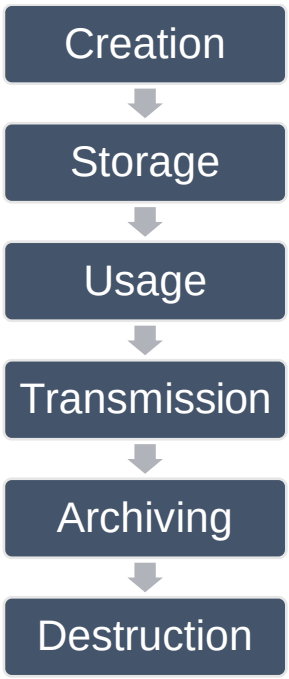
Standard Data Classification Levels

Classification Level	Definition	Examples
Level 5: [Top Secret]	Applies to data that is highly sensitive and its use should be limited on a need-to-know basis. If disclosed, there would be a significant financial, legal and/or reputational damage to the organisation.	• Personal identifiable information (PII) • Health information • Financial Data
Level 4: [Secret]	Applies to data that if compromised could negatively impact operations, including harming the organisation, its patients, partners, or employees.	• Employee Salaries/reviews • Vendor contracts
Level 3: [Protected]	Applies to data that is intended for use within the organisation. Unauthorised external disclosure could adversely affect the organisation, its patients, employees, and business partners.	• Earnings • Memos
Level 2: [Official: Sensitive]	Applies to data that is not openly published but can be made available via open record requests. Direct access to this data is restricted to authenticated and authorised employees. Limited data may contain redactions to protect confidential material.	• Policies and Procedures • Employee handbooks
Level 1: [Official]	Applies to data that is readily available to the public with anonymous access.	• Press releases • Public access website pages • Brochures
Level 0: [Unofficial]	Applies to data that is not associated with an official duty or business activity	• Non work-related emails

		• Personal opinions and ideas

Data Handling Requirements

The data lifecycle is as follows:



For data that is Level 0:[Unofficial] there are no formal handling requirements. However staff are strongly encouraged to review and evaluate whether Level 0:[Unofficial] data is accurately classified and to update labelling and handling requirements accordingly.

Data Handling Requirements Matrix

Creation

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Creation Of Data On Shared Drives	No requirement.	Ensure proper labelling immediately upon creation.	Level 2, and creation/ discussion of new data in public/on a public network is prohibited. Creation of data on a local desktop is not recommended	Level 3, and ensure all creation/ discussion is done in private with authorised personnel only.	Same as Level 4.

			as it is not backed up.		
Creation Of Data On Mobile Devices (E.G. Mobile Devices)	No requirement.	Ensure proper labelling immediately upon creation.	Level 2, and creation/ discussion of new data in public/on a public network is prohibited.	Not permitted.	Not permitted.
Creation Of Data On Any Internally Hosted Web Server	No requirement.	Ensure proper labelling immediately upon creation.	Level 2, and creation/ discussion of new data in public/on a public network is prohibited. Ensure use of secure connection (e.g. https).	Level 3, and ensure all creation/ discussion is done in private with authorised personnel only.	Level 4, and not permitted on a non-corporate network.
Creation Of Data On Any Sanctioned Third-Party Web Application (Such As Sharepoint Online)	No requirement.	Ensure proper labelling immediately upon creation (where possible). Creation of data must be approved by the appropriate data owner(s).	Level 2, and creation/ discussion of new data in public/on a public network is prohibited. Ensure use of secure connection (e.g. https).	Same as Level 3.	Same as Level 3.
Creation Of Data On Any Unsanctioned Third-Party Web Application (Such As Google Docs Or Surveymonkey)	No requirement.	Ensure proper labelling immediately upon creation (where possible). Creation of data must be approved by the appropriate data owner(s).	Not permitted.	Not permitted.	Not permitted.
Creation Of Physical Data	No requirement.	Ensure proper labelling upon creation.	Level 2, and creation/ discussion of new data in	Level 3, and ensure all creation/ discussion of data is completed in private with	Same as Level 4.

			public is prohibited.	authorised personnel only.	

Storage

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Storing Data On Local Drives	Not recommended as local drives are not backed up.	Not permitted.	Not permitted.	Not permitted.	Not permitted.
Storing Of Data On Shared Drives	Follow corporate drive storage conventions.	Level 1, and basic levels of authentication and access.	Same as Level 2.	Same as Level 2.	Level 4, and access requires two-factor authentication. Data must be password protected. Shared drives are encrypted.
Storing Data On Corporate Mobile Devices (E.G. Smartphones)	Follow corporate drive storage conventions.	Level 1, and must be managed through MDM solution. Mobile device must be password protected.	Same as Level 2.	Not permitted.	Not permitted.
Storing Data On Personally Owned Mobile Devices	Follow corporate drive storage conventions.	Mobile device must be password protected.	Mobile device must be encrypted. If the device is lost, it may be remotely wiped.	Not permitted.	Not permitted.
Storage Of Data On Any Sanctioned Third-Party Hosted Application (Such As Sharepoint Online)	Follow corporate storage conventions.	Level 1, and third party must meet security requirements set up by the IT team before being used. Basic levels of authentication	Level 2, and encrypted when stored on systems managed by a vendor performing services for the organisation.	Level 3, and vendor must log access and make logs available upon request.	Not permitted.

		and access are required.	Access must be federated.		
Storage Of Data On Any Unsanctioned Third-Party Hosted Application (Such As Surveymonkey, Google, Dropbox)	Follow corporate storage conventions.	Not permitted.	Not permitted.	Not permitted.	Not permitted.
Storage Of Data On Any Removable Media	Follow corporate drive storage conventions.	Level 1, and follow basic levels of physical security. Label removable media with appropriate classification level.	Level 2, and data owner approval required for storage on removable media. Only company-issued devices may be used.	Not permitted.	Not permitted.
Storage Of Physical Data	Follow corporate organisational standards.	Level 1, and data must be kept out of sight after hours or when visitors are present.	Level 2, and access to the facility requires centralised electronic badge access based upon least privilege. Access is reviewed regularly.	Level 3, and data must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer when not attended by an authorised user. Storage location must provide 24/7 video surveillance.	Level 4, and locked storage must require two-factor authentication.

Usage

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Accessing Of Data On Shared Drives	Follow standard user authentication practices in place for remote access to	Level 1, and VPN access is required for remote access. Data is not permitted to be	Level 2, and two-factor authentication is required for all remote access.	Level 3, and file/ folder access is provisioned to select users.	Level 4, and no remote access is permitted.

	systems hosting the data (username and password).	accessed from a public network.			
Posting Of Data On Public Website	Permitted only by approved by posters.	Level 1, and permitted only after formal reclassification from "limited" to "public" classification.	Not permitted.	Not permitted.	Not permitted.
Posting Of Data On Social Media	Follow standard practices aligning with the Social Media Acceptable Use Policy.	Level 1, and permitted only after formal reclassification from "limited" to "public" classification.	Not permitted.	Not permitted.	Not permitted.
Printing And Other Use Of Physical Data	Follow standard practices aligning with the Printing Acceptable Use Policy. Printed data must follow storage requirements of physical data.	Level 1, and data should only be printed/copied internally or to satisfy an open records request.	Level 1, and data should only be printed when there is a legitimate business need.	Level 3, and employees should use “Follow-Me” printing to ensure copy is not picked up by unauthorised person. Copies must only be shared with individuals with authorised clearance. Copies must be marked as appropriate (e.g. “Confidential”). All usage must be performed in private.	Level 4, and all copies must be numbered and tracked.

Transmission

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Emailing Of Data Internally	Follow standard practices aligning with the Email Acceptable Use Policy.	Level 1, and the email shall include a statement identifying the classification level and list	Same as Level 2.	Level 3, and data must be password-protected and encrypted, without the password in the same email.	Level 4, and the email classification must also be labelled in the subject line. Sending of Level 5 data

		restrictions for redistribution. If transmitting in response to open records request, ensure proper redactions are applied. Attention must be paid to verify recipient information to avoid unintentional information disclosure.		Transmission by non-encrypted email is prohibited. The email shall include a statement identifying the classification level and list restrictions for redistribution.	should be kept to a minimum and must be approved by the appropriate data owner(s).
Emailing Data Externally To Sanctioned Third Parties (Such As Customers And Partners)	Follow standard practices aligning with the Email Acceptable Use Policy.	Level 1, and the email shall include a statement identifying the classification level and list restrictions for redistribution. If transmitting in response to open records request, ensure proper redactions are applied. Attention must be paid to verify recipient information to avoid unintentional information disclosure.	Same as Level 2.	Level 3, and data must be password-protected and encrypted, without the password sent through email. Transmission by non-encrypted email is prohibited. The email shall include a statement identifying the classification level and list restrictions for redistribution. Sending of data must be approved by the appropriate data owner(s).	Level 4, and the email classification must also be labelled in the subject line. Sending of data should be kept to a minimum and must be approved by the appropriate data owner(s).
Emailing Data Externally To Unsanctioned Third Parties (Such As Auto-Forwarding To Personal Email, Friends)	Follow standard practices aligning with the Email Acceptable Use Policy.	Level 1, and not permitted unless formal reclassification and redaction (e.g. Open Requests Request).	Not permitted.	Not permitted.	Not permitted.

Other File Sharing Platforms	Follow standard practices aligning with the relevant Acceptable Use Policy.	Level 1, and file sharing must be through approved platforms, such as corporate accounts for OneDrive or SFTP. There must be a legitimate business need for file sharing at this level. Non-sanctioned platforms are not permitted for file sharing.	Level 2, and documents must be password protected in the approved sharing platform.	Level 3, and file sharing at this level is on a need-to-know basis only.	Same as level 4.
Granting Permission To View, Write, Or Edit Data Internally	No requirement.	Read, write, and/or edit access will be dictated by role-based access.	Level 2, and employees can decide if other employees need to be granted access to data.	Level 3, and read, write, and/or edit access is not permitted, unless approved by the appropriate data owner(s) Read, write, and/or edit access will be dictated by role-based access. Read access may be provisioned, while write/edit access is typically not recommended.	Same as Level 4.
Granting Permission To View, Write, Or Edit Data Externally (I.E. Third Parties)	No requirement.	Request for information to be shared externally must be through proper channels (Open Records Request).	Level 2, and third party must sign a nondisclosure agreement (NDA) and adhere to the organisation's data handling standard. Data owner must approve third-party	Level 3, and the IT security team should be involved in vetting third party to ensure it meets internal requirements. Audit third party for their data handling practices.	Same as Level 4.

			handling of this data.	Must be legitimate need for information.	
Sending Of Physical Data	Follow standard mailing conventions.	Level 1, and not permitted unless formal reclassification and redaction if externally sent (e.g. Open Records Request).	Physical media transport should be limited to small amounts of sensitive materials and sent only through an accountable commercial delivery service, if applicable. A cover letter should include a statement identifying the classification level and list restrictions for redistribution.	Level 3, and physical media transport is discouraged and should be limited to small amounts of sensitive materials. It should be sent only through an accountable commercial delivery service. Receipt must be confirmed and logged. The cover letter shall include a statement identifying the classification level and list restrictions for redistribution.	Level 4, and/or physical media should be transported by internal authorised personnel. Receipt must be confirmed and logged. The cover letter shall include a statement identifying the classification level. Explicit clearance for redistribution is required.

Archiving

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Archiving Of Data Onsite	Archiving follows the established backup schedule, as found in the Backup and Recovery Policy Storage of data is kept the same as dictated in the storage requirements for Level 1.	Archiving follows the established backup schedule, as found in the Backup and Recovery Policy Storage of data is kept the same as dictated in the storage requirements for Level 2.	Archiving follows the established backup schedule, as found in the Backup and Recovery Policy. Storage of data is kept the same as dictated in the storage requirements for Level 3.	Archiving follows the established backup schedule, as found in the Backup and Recovery Policy Storage of data is kept the same as dictated in the storage requirements for Level 4.	Archiving follows the established backup schedule, as found in the Backup and Recovery Policy Storage of data is kept the same as dictated in the storage requirements for Level 5.
Archiving Of Data To A Backup	Ensure that third party follows Level 1	Ensure that third party follows Level 2	Ensure that third party follows Level	Ensure that third party follows Level 4 data archiving	Ensure that third party follows Level

Provider Or Cloud Service	data archiving and storage requirements.	data archiving and storage requirements.	3 data archiving and storage requirements.	and storage requirements.	5 data archiving requirements.
Archiving Of Physical Data	Backups recommended at an offsite facility.	Level 1, and ensure physical security of the offsite facility with centralised management of key disbursements.	Level 2, and centralized electronic badge access based upon least privilege.	Level 3, and camera coordination for events. Storage location must provide 24/7 video surveillance.	Level 4, and two-factor authentication s required for access.

Destruction

	LEVEL 1 [OFFICIAL]	LEVEL 2 [OFFICIAL: SENSITIVE]	LEVEL 3 [PROTECTED]	LEVEL 4 [SECRET]	LEVEL 5 [TOP SECRET]
Destruction Of Data And Files	Follow standard file deletion process in accordance with the Information Retention Policy.	Level 1, and verify that backups and alternate copies have been destroyed, if applicable.	Level 2, and maintain a record of disposal.	Same as Level 3.	Same as Level 3.
Destruction Of Data Storage Devices (E.G. Hard Drives, Usbs)	Follow standard hardware destruction practices in accordance with the Hardware Asset Management Policy.	Same as Level 1.	Level 1, and maintain a record of disposal.	Level 3, and hardware must be degaussed, disintegrated, and/or incinerated.	Level 3, and hardware may be degaussed, followed by disintegration and/or incineration.
Destruction Of Data On Third-Party Hosted Services	Follow standard data deletions practices.	Level 1, and verify that the third party adheres to internal data destruction requirements.	Level 2, and maintain a record of disposal.	Same as Level 3.	Same as Level 3.
Destruction Of Physical Data	Follow local garbage/ recycling guidelines.	Level 1, and shred paper documents.	Records should be cross-shredded and/or incinerated. Maintain a record of disposal.	Same as Level 3.	Same as Level 3.

Electronic Disclaimers and Restrictions

Sample disclaimers and statements to include in electronic messages, such as emails and log-in banners, containing information that has been classified in accordance with [organisation's] Data Classification Policy and Standard are included in the table below. For officially sensitive, protected, secret, or top secret data, the classification should be included in the subject line in all capital letters (e.g. OFFICIAL:SENSITIVE, PROTECTED SECRET, or TOP SECRET). This label alerts the recipient to the level of care and restriction required.

Classification	Sample Disclosure Statements for Electronic Data
Level 5	**Level 5:** This email and any attachments contain information that has been classified as "[**TOP SECRET**]." It is intended exclusively for the use of the individual(s) to whom it is addressed. If inappropriately disclosed, this information could result in grave danger to corporate and/or national security, as well as be hazardous to the life, health, or financial situation of the individual(s) or organisation(s) identified in this email. This information may be protected by federal and state laws or regulations. Retransmission or forwarding of this email is forbidden without explicit written approval from the data custodian. The data must only be stored in encrypted format and cannot be taken off the network. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or its contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.
Level 4	**Level 4:** This email and any attachments contain information that has been classified as "[**SECRET**]." It is intended exclusively for the use of the individual(s) to whom it is addressed. If inappropriately disclosed, this information could be hazardous to the life, health, or financial situation of the individual(s) or organisation(s) identified in this email. This information may be protected by federal and state laws or regulations. Retransmission or forwarding of this email must only be done after notifying the data custodian. The data must only be stored in encrypted format. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.
Level 3	**Level 3:** This email and any attachments contain information that has been classified as "[**PROTECTED**]." It is intended exclusively for the use of the individual(s) to whom it is addressed. Information that is only available to internal authorised users is contained within and may be protected by federal and state laws or regulations. Retransmission or forwarding of this email must only be done when properly encrypted and only to authorised individuals. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or its contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.
Level 2	**Level 2:** This email and any attachments contain information that has been classified as "[**OFFICIAL: SENSITIVE**]" distribution and is intended solely for the use of the individual(s) to whom it is addressed. It should be

	retransmitted or forwarded only to individuals authorised to receive such information. If you are not the intended recipient, you may not use, copy, distribute, or forward this message or contents to anyone. If you have received this email in error, please notify the sender immediately and delete the email from your email system.
Level 1	No disclaimer or statement required but labelling as "[**OFFICIAL**]" is recommended
Level 0	No disclaimer or statement required.

Physical Disclaimers and Restrictions

Sample disclaimers and statements to include along with any mailings or transmission of physical, hard copy information that has been classified in accordance with [organisation's] Data Classification Policy and Standard are included in the table below. For officially sensitive, protected, secret, or top secret data, the classification should be included in the subject line in all capital letters (e.g. OFFICIAL:SENSITIVE, PROTECTED SECRET, or TOP SECRET). This label alerts the recipient to the level of care and restriction required.

Classification	Sample Disclosure Statements for Physical/Mail Data
Level 5	**Level 5:** This document and any attachments contain information that has been classified as "**[TOP SECRET]**" and is intended solely for the use of the individual(s) to whom it is addressed. It contains data whose inappropriate disclosure could result in grave danger to corporate and/or national security, as well as be hazardous to the life, health, or financial situation of the individual(s) or organisation(s) identified in this document. It contains information that may be protected by federal and state laws or regulations. Receipt must be confirmed and logged. This data may only be released through a formal legal process. It should NOT be copied or redistributed without explicit written approval from the data custodian responsible for this data. This document and any attachments must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer, when not attended by an authorised user. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately.
Level 4	**Level 4:** This document and any attachments contain information that has been classified as "[**SECRET**]" and is intended solely for the use of the individual(s) to whom it is addressed. It contains data whose inappropriate disclosure could be hazardous to the life, health, or financial situation of the individual(s) or organisation(s) identified in this document. It contains information that may be protected by federal and state laws or regulations. Receipt must be confirmed and logged. This data may only be released through a formal legal process. It should not be copied or redistributed without contacting the data custodian responsible for this data.

	This document and any attachments must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer, when not attended by an authorised user. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately.
Level 3	**Level 3:** This document and any attachments contain information that has been classified as "[**PROTECTED**]" and is intended solely for the use of the individual(s) to whom it is addressed. It contains information that is available only to internal authorised users and may be protected by federal and state laws or regulations. This data may only be released through a formal legal process. It should be redistributed or forwarded only to individuals authorised to receive such information. This document and any attachments must be stored in a secure environment or locked compartment, such as a filing cabinet or desk drawer, when not attended by an authorised user. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately and destroy this document and all attachments.
Level 2	**Level 2**: This document and any attachments contain information that has been classified as "[**OFFICIAL:SENSITIVE**]" distribution and is intended solely for the use of the individual(s) to whom it is addressed. It should be redistributed or forwarded only to individuals authorised to receive such information. If you are not the intended recipient, you may not use, copy, distribute, or forward this document, its content, or its attachments to anyone. If you have received this document in error, please notify the sender immediately and destroy this document and all attachments.
Level 1	No disclaimer or statement required but labelling as "[**OFFICIAL**]" is recommended.
Level 0	No disclaimer or statement required.

Related Documents

- Information Security Policy Charter
- Data Classification Policy