

## Document History

### Revision History

Revision Date	Revision Number	Summary of Changes	Changes Marked
31/01/22	2.0	Updated Version	Y
02/05/23	3.0	Major update to classification matrix, handling guidelines and inclusion of the category of OFFICIAL-SENSITIVE: SNI category	N
04/05/23	3.1	Minor updates to OFFICIAL-SENSITIVE: SNI	Y
11/09/23	3.2	Inclusion of the Data Retention Policy	Y
04/03/24	4.0	Update for 2024	Y
17/03/25	5.0	Updated for ISO27001:2022 controls, simplified the classifications matrix	Y

### Distributed for Review

This document has been distributed for the following to review:

Name	Title	Company	Issue Date
Hitesh Chavda	Chief Information Officer	Mitie	12/03/24
Katherine Woods	Deputy Group Legal Counsel	Mitie	12/03/24
Tyler Regan	Director IS Service Management	Mitie	12/03/24
Daniel Waddy	Senior Information Security Consultant	Mitie	12/03/24
Ian Cotterill	Senior Information Security Auditor	Mitie	12/03/24
Chris Gould	Data Privacy Director	Mitie	12/03/24
David Grant	CG&D Data Controller	Mitie	12/03/24

### Approvals

This document requires the following approvals:

Name	Title	Issue Date	Revision
John Cruise	Chief Information Security Officer	17/03/24	5.0

## Contents

Document History.....	1
Revision History .....	1
Distributed for Review.....	1
Approvals.....	1
Purpose.....	3
Scope.....	3
Classifications .....	3
Responsibilities.....	4
Information Owners .....	4
Users.....	5
Information Custodians.....	5
Classification and Guidance .....	5
Storage and Transmission.....	6
Data Destruction – General Guidance .....	6
Information Access .....	6
Classification Matrix .....	7
Information Handling Matrix - Commercial .....	10
Information Handling matrix - HMG Classification .....	11
Data Retention Policy .....	13
Appendix .....	18
Controls within this policy.....	18
Definitions.....	18
Exceptions.....	18
Support .....	18

## Purpose

The purpose of this policy is to provide information that will help anyone handling Mitie information assets so that they can provide the appropriate level of protection according to the significance and sensitivity classification of the information.

Information security classifications and associated protective measures are needed to help balance both the business needs to share or restrict information, and the business impacts associated with any unauthorised access or damage to the information.

They seek to ensure that the following business needs are met:

- **Confidentiality:** To protect sensitive information from unauthorised disclosure or interception.
- **Integrity:** To safeguard the accuracy and completeness of information and computer data.
- **Availability:** To ensure information is accessible and useable when required for authorised use

## Scope

This policy applies to all Mitie information however it is produced or stored and all users of Mitie information.

Everyone who is covered by the scope of this procedure has a responsibility to comply with the requirements. By agreeing to do this, you will be helping to protect the information and services that Mitie relies upon to operate its business safely, maintain our customers' confidence and keep our jobs secure.

## Classifications

Mitie information assets must be classified appropriately under one of five categories. This is so the information can be handled and protected to a level that is appropriate to the sensitivity and value of the information to Mitie. The five categories are:

- PUBLIC
- INTERNAL
- CONFIDENTIAL
- HIGHLY CONFIDENTIAL
- OFFICIAL
- OFFICIAL-SENSITIVE
- OFFICIAL-SENSITIVE:SNI

The OFFICIAL & OFFICAL-SENSITIVE data classifications are restricted to the storage and processing of information for Ministry of Defence and Central Government departments. This information can only be stored on approved systems and accessed by staff who are appropriately cleared.

OFFICIAL-SENSITIVE:SNI data classification is restricted to the processing and storage of information on behalf of the Nuclear Decommissioning Agency. This information can only be processed at the approved facility which is currently:

Mitie Total Security Management  
Pavilion Drive,  
Northampton Business Park,  
Brackmills,  
Northampton,  
NN4 7SL

This procedure will provide information to help anyone handling Mitie information determine what category their information comes under and what they need to do to appropriately protect the information.

## Responsibilities

To facilitate the protection of information, responsibilities towards information must be established at three levels:

## Information Owners

The Owner is the management of an organisational unit, department, or team where the information is created, or where they are the primary user or beneficiary of the information. The Owner is ultimately responsible for:

- Knowing and understanding the information for which they are responsible.
- Evaluating and ensuring the data has been appropriately classified, based on legal and regulatory requirements, any contractual obligations and this Information classification policy
- Establishing how long the information should be retained; in either or both hardcopy and softcopy EG:- Online, in IT Systems, Offline, on backup, vaulting or archive media
- Retention limits should be set in accordance with either client requirements or the legal and contractual requirements.
- Ensuring that personally identifiable information is protected in line with the Mitie Data protection policies.
- Establishing criteria for access to and usage of information; this can include delegating responsibility for authorisation and revoking access to the information
- Exercising due care in the setting of standards for protection of the information
- Monitoring compliance to and enforcing this policy
- Reporting any non-compliance situations or events to the Mitie Information Security team
- Note: Responsibility for implementing security measures may be delegated, but accountability will remain with the assigned owner of the information asset.

## Users

A User is an employee, contractor or 3rd party that has been authorised by the Information Owner to access information and use the safeguards established by the Information Owner. Being granted access to information does not imply or confer authority to grant other users access to that information. A User is responsible for:

- Following information access and processing procedures established by the Information Owners.
- Accessing only the information for which they are authorised.
- Reporting suspected or actual violations of policies and standards to the Information Owner.
- Exercising due care in the use of personally identifiable information in accordance with the Mite data protection policies.

## Information Custodians

The Custodian is an employee, contractor or 3rd party who is in possession of the information and is responsible for managing the systems (or media) that host the information belonging to the Information Owner. An Information Custodian is responsible for:

- Executing access controls, safeguards and data transfers and exchanges that have been authorised by the Information Owner
- Using best practices to maintain the confidentiality, integrity, and availability of information
- Exercising due care in the administration of systems storing or processing the Information
- Protecting information in accordance with this information classification policy
- Exercising due care in the use of sensitive data in compliance with the Mite data protection policies.

## Classification and Guidance

The requirements when classifying information include:

- All Mitie information must be clearly labelled to advertise which category it is so that anyone who handles the information can handle it appropriately.
- Only Mitie's Group Marketing and Communications Team may classify documents / information as "PUBLIC";
- The owner of the Information (e.g. author of a document) is responsible for its correct classification. They have to evaluate the information asset's security relevance and also determine the distribution list according to the "need to know" principle;
- Unlabelled documents/information have to be considered at least as "CONFIDENTIAL";
- In case of doubt about the correct level of classification, the higher security level should be chosen. If the document is composed from several single components with different security relevance, the highest security level must be chosen;
- Information that Mitie receives from 3rd parties that is declared as CONFIDENTIAL should be classified internally as CONFIDENTIAL. It may be forwarded only with explicit approval of the 3rd party (e.g. to other 3rd parties);
- All documentation front pages and/or document header /footers should include one of the classifications listed above.
- Classification must be re-evaluated when changes are made to the documentation, for example a template will have a lower classification than when it is completed with personal information;

- All managers are directly responsible for implementing this policy within their business areas, and for ensuring their staff, suppliers and third parties adheres to these requirements.
- Data classified as OFFICIAL or OFFICIAL-SENSITIVE is HMG protectively marked and must only be stored and processed within the UK or designated overseas territories (military bases and Foreign, Commonwealth & Development Office)
- Data classified as OFFICIAL-SENSITIVE:SN1 is marked by the Office for Nuclear Regulation and can only be processed at the Northampton office.

## Storage and Transmission

Mitie store all electronic documentation in Microsoft Office 365, located in the Microsoft UK tenant and has full encryption enabled by default using AES 256

Non-document information is stored within the production applications, these are hosted in Microsoft Azure or Amazon Web Services. All data is encrypted at rest using AES 256.

All data transmissions are encrypted using TLS 1.2 or TLS 1.3

## Data Destruction – General Guidance

All physical documents must be disposed of in accordance with the handling matrix listed below. The confidential waste bin in all Mitie offices is managed through a contract with Shred-It. Shred-It provide confidential disposal in accordance with Information Assurance Standard 5, certificates of destruction are available.

Destruction of physical media and infrastructure is managed by a contract with SCC who will destroy this in accordance with Information Assurance Standard 5. To arrange destruction of physical media or devices please log a ticket with the service desk or see your local on-site support. A certificate of destruction is available.

## Information Access

Access to information in Mitie is restricted based on Role Based Access Control and justified requirement. To access any information, you must have a Mitie device that is joined to the Azure Active Directory and a successful Multi Factor Authentication challenge. Multi Factor Authentication is restricted to Microsoft Authenticator or Yubico FIDO2 key.

## Classification Matrix

The matrix below provides example information assets and the information classification that they should normally receive.

Classification	Security Relevance	Description	Data Documents
<b>PUBLIC</b>	Relevance is “Low” Items are: <ul style="list-style-type: none"> <li>• freely accessibly</li> <li>• generally – known</li> <li>• possibly published</li> </ul>	<ul style="list-style-type: none"> <li>• Information that can be disclosed to anyone without violating an individual’s right to privacy. Knowledge of this information does not expose the company to financial loss or embarrassment</li> <li>• Information approved for external dissemination by Mitie’s Group Marketing and Communications Team to the general public.</li> </ul>	<ul style="list-style-type: none"> <li>• Mitie public website content</li> <li>• Marketing brochures</li> <li>• Customer disclosure statements</li> <li>• Published annual reports</li> <li>• Press releases / Interviews with news media</li> </ul>
<b>INTERNAL</b>	Relevance is “Medium” Items are: <ul style="list-style-type: none"> <li>• Internally freely accessibly</li> </ul>	<ul style="list-style-type: none"> <li>• Information intended for use only within the company. Unauthorised disclosure, compromise, or destruction would not have a significant impact on the company, its employees or customers.</li> <li>• Contractors and temporary employees who have signed confidentiality agreements may also be given access to this information</li> </ul>	<ul style="list-style-type: none"> <li>• Policies</li> <li>• Training material</li> <li>• Organisation charts</li> <li>• Procedures and instructions without confidentiality restrictions</li> <li>• Internal blank forms (for instance an employee appraisal form template – with no information entered)</li> </ul>

Classification	Security Relevance	Description	Data Documents
<b>CONFIDENTIAL</b>	<p>Relevance is “High” The Items -</p> <ul style="list-style-type: none"> <li>• Have limited Access</li> <li>• Are knowledge person bound</li> </ul>	<ul style="list-style-type: none"> <li>• Information that the Company has a legal, regulatory, or commercial requirement to protect. It is intended for use solely within defined groups in the company.</li> <li>• Unauthorised disclosure, compromise or destruction would adversely impact the company, its employees or customers</li> <li>• This information must be handled in such a way that no 3rd parties outside Mitie can have access to it in any form, unless non-disclosure agreements are in place.</li> </ul> <p><b>Sensitive information</b></p> <ul style="list-style-type: none"> <li>• Information that the Company has a legal, regulatory, or social obligation to protect. It is intended for use solely within defined groups in the company.</li> <li>• Unauthorised disclosure, compromise or destruction would adversely impact the company, its employees or customers</li> <li>• This information must be handled in such a way that no 3rd parties outside Mitie can have access to it in any form, unless non-disclosure or DPA (if relating to personal information) agreements are in place.</li> </ul>	<ul style="list-style-type: none"> <li>• Information provided by or relating to Mitie's customers</li> <li>• Sensitive legal or contractual information</li> <li>• Contracts, price agreements Employee appraisal forms once completed</li> <li>• Mitie Technical design documents</li> <li>• IT system audit records, log files</li> <li>• Application source code and configuration files</li> <li>• PII Data – as defined by the ICO</li> </ul> <p><b>Sensitive information</b></p> <ul style="list-style-type: none"> <li>• Customer data</li> <li>• Bank details</li> <li>• Employee data</li> <li>• Salary information</li> <li>• Ethnicity</li> <li>• Health records</li> <li>• Sensitive customer data</li> </ul>
<b>HIGHLY CONFIDENTIAL</b>	<p>Relevance is “Very High” The Items –</p> <ul style="list-style-type: none"> <li>• have restricted access</li> <li>• are knowledge person bound</li> </ul>	<ul style="list-style-type: none"> <li>• Information and documents which can threaten the existence of Mitie or a Mitie premises</li> <li>• Information that is made available on an explicit pre-determined need-to-know basis or that requires special protection due to the nature of the information.</li> <li>• Restricted information may not be removed from Mitie facilities without written consent of the Data Owner and or Senior Management</li> </ul>	<ul style="list-style-type: none"> <li>• Strategic plans</li> <li>• Financial Performance Information</li> <li>• Financial budgets</li> <li>• Special Category PII data – as defined by the ICO</li> <li>• Cryptographic private and non-public keys for business IT systems</li> <li>• Certification authority signing keys for IT systems</li> </ul>

Classification	Security Relevance	Description	Data Documents
<b>OFFICIAL</b>	Relevance is “High” The Items – <ul style="list-style-type: none"> <li>• Have limited Access</li> <li>• Are knowledge person bound</li> </ul>	<ul style="list-style-type: none"> <li>• Information is protectively marked in line with HMG marking scheme – May 2018_GovernmentSecurity-Classifications-2.pdf (<a href="http://publishing.service.gov.uk">publishing.service.gov.uk</a>)</li> <li>• The information may not be marked, however, anything from HMG (Central Government, Ministry of Justice or Ministry of Defence) must be assumed to be classified as OFFICIAL at a minimum.</li> <li>• Data must only be stored and processed within the UK</li> </ul>	<ul style="list-style-type: none"> <li>• General documents and data from HMG</li> </ul>
<b>OFFICIAL SENSITIVE</b>	Relevance is “Very High” The Items – <ul style="list-style-type: none"> <li>• Have restricted access</li> <li>• require SC Clearance</li> </ul>	<ul style="list-style-type: none"> <li>• Information is protectively marked in line with HMG <u>marking scheme</u> – <a href="http://publishing.service.gov.uk">May 2018_GovernmentSecurity-Classifications-2.pdf (publishing.service.gov.uk)</a></li> <li>• Data must only be stored and processed within the UK</li> <li>• Mandatory TLS email encryption must be used</li> </ul>	<ul style="list-style-type: none"> <li>• Restricted OFFICIAL category of data</li> </ul>
<b>OFFICIAL SENSITIVE:SN1</b>	Relevance is “Very High” Items <ul style="list-style-type: none"> <li>• Have restricted access</li> <li>• require SC Clearance</li> </ul>	<ul style="list-style-type: none"> <li>• Information is protectively marked inline with Office for Nuclear Regulation (ONR) – <a href="http://onr.org.uk">NSR 2003 – Classification Policy for the Civil Nuclear Industry (onr.org.uk)</a></li> <li>• Must only be processed at the following address:                Mitie Total Security Management                Pavilion Drive                Northampton Business Park                Brackmills                Northampton                NN4 7SL</li> <li>• Physical data must only be stored at the above address</li> </ul>	<ul style="list-style-type: none"> <li>• Information related to the Office for Nuclear Regulation and Nuclear Decommissioning Agency</li> </ul>

### Information Handling Matrix - Commercial

The Matrix below provides recommended ways to store Mitie information depending on the type of storage and classification of the information.

Mitie Classification	Electronic Storage	Physical Storage	Electronic Distribution	Physical Distribution	Recommended Disposal
<b>PUBLIC</b>	Mitie Commercial Office 365 general storage	In general office environment	Mitie general Office 365	Normal mail for external posting	Dispose of documents within the confidential waste bins at the local office
<b>INTERNAL</b>	Mitie Commercial Office 365 general storage	In office environment using lockable drawers or cupboards	Mitie general Office 365	Normal mail for external posting	Dispose of documents within the confidential waste bins at the local office
<b>CONFIDENTIAL</b>	Mitie Commercial Office 365 general storage	In office environment using lockable drawers or cupboards	Mitie general Office 365	Use sealed envelope with tracking	Dispose of documents within the confidential waste bins at the local office
<b>HIGHLY CONFIDENTIAL</b>	Mitie Commercial Office 365 restricted storage	Stored in physically and environmentally secure environment such as a data safe	Mitie Office 365 platform with additional encryption controls.	Use sealed envelope sent either via Royal Mail special delivery or confidential courier	Dispose of documents within the confidential waste bins at the Birmingham, Bristol, Manchester, London, or Northampton office

### Information Handling matrix - HMG Classification

The Matrix below provides recommended ways to store information that has specific HMG classification and is general guidance. Where a specific Security Aspects Letter has been issued, the table of handling instruction specific to that contract must be used.

Mitie Classification	Electronic Storage	Physical Storage	Electronic Distribution	Physical Distribution	Recommended Disposal
<b>OFFICAL</b>	Data can be stored within the Commercial Mitie Office 365 environment – Email, Teams, OneDrive	In lockable drawers or cupboards.	Standard Mitie E-mail & Teams	Use sealed envelope with tracking. The outside of the envelope must be plain. It must not contain the classification of the information	Dispose of documents within the confidential waste bins at the local office
<b>OFFICAL - SENSITIVE</b>	Data can be stored within the Commercial Mitie Office 365 environment – Email, Teams, OneDrive	Lockable and secured filing cabinet at Birmingham, Bristol, Manchester, London, or Northampton office	Mitie Commercial email and Teams can be used internally. The sender must validate that the recipients are correctly security cleared and are using the restricted Mitie Commercial Office 365. Using the sec.mitie.co.uk Office 365 service – all recipients are already SC cleared	Use sealed envelope sent either via Royal Mail special delivery or confidential courier. The outside of the envelope must be plain. It must not contain the classification of the information	Dispose of documents within the confidential waste bins at the Birmingham, Bristol, Manchester, London or Northampton offices

Mitie Classification	Electronic Storage	Physical Storage	Electronic Distribution	Physical Distribution	Recommended Disposal
<b>OFFICIAL SENSITIVE: SNI</b>	Data can only be stored within the restricted Mitie Commercial SharePoint or within the sec.mitie.co.uk Defence / Government Office 365 environment	Lockable and secured filing cabinet at the Northampton office	<p>Must be restricted to approved internal staff who are SC Cleared and approved for handling Sensitive Nuclear Information.</p> <p>Must not be sent externally – except to the Nuclear Decommissioning Authority or the Office for Nuclear Regulation. All email must be sent using Egress, this ensures full encryption of the email and contents</p>	Use sealed envelope sent either via Royal Mail special delivery or confidential courier. The outside of the envelope must be plain. It must not contain the classification of the information	Dispose of documents within the confidential waste bins at the Northampton office.

## Data Retention Policy

Record Type	Specific Record	Retention Period
<b>Customer Data</b>	Non-document data retained with Mitie applications	Unless specified in the contract with the customer data will be retained for 6 years or the lifetime of the contract (whichever is shorter) plus 6 months from contract termination.
	Document data that is not covered under <b>Agreements and other related correspondence</b> section	Unless specified in the contract with the customer, data will be retained for 6 years or the lifetime of the contract (whichever is shorter) plus 6 months from contract termination.
<b>Property Documents</b>	Deeds of title	Until sold or transferred from / with company.
	Leases	15 years after termination and any terminal queries.
	Reports and opinions	10 years after last correspondence.
	Property files and related documentation	Life of company.
<b>Agreements and Other Related Correspondence</b>	Contracts with customers, suppliers, or agents	6 years after expiry of termination of the contract. Note that if the contract is executed as a deed, the period is 12 years. Action for latent damage may be brought up to 15 years after the damage occurs. PFI contract information to be retained for 30 years.
	Licensing Agreements	6 years after expiry of termination of the contract.
	Rental and Hire Purchase	6 years after expiry of termination of the contract.
	Indemnities, guarantees, bonds and similar agreements and documents	6 years after expiry of termination of the contract. Action for latent damage may be brought up to 15 years after the damage occurs.
	Other agreements/contracts	6 years after expiry of termination of the contract.
<b>Accounting and Tax Records</b>	Company accounts (including subsidiary accounts making up a Group account)	For PLC's 6 years from the year end (this includes subsidiaries of the PLC).
	Supporting information for VAT purposes	6 years or to the end of an enquiry if an enquiry lasts greater than 6 years.
	Supporting information for corporation tax calculations	6 years from the end of the period for which the company may be required to deliver a tax return, or, if longer, to the end of an enquiry.
	Supporting information for PAYE payments	PAYE records not required to be sent to HMRC to be kept for 3 years.
	All statutory records e.g., sickness, SMP, SAP, SPP, SLR	3 years after the end of the tax year.

Record Type	Specific Record	Retention Period
<b>Accounting and Tax Records (continued)</b>	Transaction related documents: sales invoices and credit notes sales ledgers Statements Purchase invoices Credit notes Cheque authorisation requests BACS reports Tender invitations to subsidiaries and bids Delivery notes and GRN's Orders	6 years from the end of the period to which the transaction relates.
<b>Bank Records</b>	Bank statements Cancelled cheques Paying in evidence Instructions to banks	6 years after year to which they relate for instructions, 6 years from the date they cease to be effective.
<b>Company Records</b>	Certificate of Incorporation	Permanently.
	Certificate to commence business Board minutes (signed copies) Minute books Board committee minutes Statutory report & accounts for Group and Company (signed copy) Resolutions passed Memorandum and Articles of Association and similar documents (signed copies) Register of seals Register of Directors' interests	<i>Note that the Company Secretarial department maintains retention details for more specific company related documents</i>
	Sale and purchase agreements on acquisitions and disposals and similar transactions	Permanently (i.e., life of the company)
	Trust deeds	12 years from redemption
	Shareholder circulars	12 years minimum
	Director representations (e.g., for auditors, statutory declarations such as internal controls sign off, etc.)	6 years from the end of the period to which the representations represent
<b>Employee Records</b>	Staff personal records (including screening certificates)	6 years after employment ceases Note: Where screening to BS7858 - 7 years after employment ceases. Note: For CCSIW - Where records are held in Wales 40 years after employment ceases.
	Payroll / wages (including PAYE related documents) Records used to calculate gross to net (including timesheets)	6 years from the end of the tax year.
	Documentation relating to identification checks under the Asylum and Immigration Act	2 years after employment ceases.
	Expense accounts	6 years.
	Labour Agreements (e.g. union related)	Permanently.
	Accident book	3 years from the date of each entry.

Record Type	Specific Record	Retention Period
<b>Employee Records (continued)</b>	Health and safety records	3 years. Note that where employees are exposed to hazardous substances this should be extended to 40 years if linked to a personal exposure record. Note that if a radiation dosimetry record, this should be extended to 50 years.
	Awards relating to accident or injury at work	12 years.
	Application forms	For duration of employment plus 6 months.
	References received	1 year.
	Annual leave records	For duration of employment plus 6 months.
	Unpaid leave / special leave records	For duration of employment plus 6 months.
	Appraisal / assessment records	For duration of employment plus 6 months.
	References given	1 year from date reference given.
	Applications from unsuccessful candidates	6 months.
	Records relating to promotion, transfer, training, or disciplinary matters	For duration of employment plus 6 months.
<b>Pensions Records</b>	All trust deeds and rules Trustees' minute books Annual accounts of funds and HMRC approvals Actuarial valuations Contribution records	Permanently.
	Money purchase details	6 years after transfer or value taken.
	Group health policies	12 years after cessation of benefit.
<b>Insurance</b>	Policies	10 years after lapse.
	Claims correspondence	5 years after settlement.
	Employer's liability certificate	40 years.
<b>QHSE Records</b>	Management reviews / KPI's Audit reports	3 years.
	Customer feedback / complaints Approved supplier / sub-contractor lists Consignment / Waste transfer notes Risk assessments	3 years, but up to 40 years if for occupational health surveillance.
	Health surveillance: Active / reactive monitoring	Up to 40 years if for occupational health surveillance.
	Incident reports	If the incident relates to an incident that has a potential PL or EL liability a minimum of 6 years.
	Mitie owned equipment records	Life of the equipment.

Record Type	Specific Record	Retention Period
<b>QHSE Records (continued)</b>	Statutory tests and certificates for equipment machinery and such like (e.g., lifting gear)	Until next certificate issued. <i>Note that if documentation is critical to investigations, maintain for 3 years after completion of investigation / settlement.</i>
<b>Food Safety</b>	Daily due diligence records Delivery monitoring records Food management & control Temperature records Top side pre-service briefs Cleaning records Temperature probe records	3 months.
<b>Security</b>	Incident reports	If the incident relates to an incident that has a potential PL or EL liability a minimum of 6 years.
<b>Systems</b>	Records in respect of contracts, including survey, design, quotations, amendments, system records, commissioning, handover documents and where appropriate	Life of contract plus 2 years.
	Maintenance, disconnection, historical and false alarm records	3 years post-corrective maintenance.
	I&HAS corrective maintenance form	
<b>MiTEC</b>	Contracts and agreements for alarm/CCTV monitoring, including actions to be taken, reporting arrangements and any amendments	Life of the contract plus 3 years as a minimum (BS5979).
	Records of all MiTec monitored events	3 years after the event to which they refer.
	Telephone communications with voice and date  Where voice communication is the subject of an enquiry	3 months after date of communication. 3 months or until the conclusion of the enquiry, whichever is the longer.
	Contract reviews	Contract life plus 2 years.
	Data communications to and from the ARC CCTV images under BS8418	12 months after the date of generation Retention times to be agreed and assessed with the owner and be in accordance with the DPA.
	Maintenance and emergency service logs	3 months or until the next service/maintenance whichever is longest.
	Daily and weekly checks	1-month minimum.
	<b>SIA</b>	All documents used within the identity verification process must be originals and authenticated copies (i.e., dated and signed to confirm the original has been seen)

Record Type	Specific Record	Retention Period
<b>Screening</b>	All documentation relating to the BS7858 screening process. <ul style="list-style-type: none"> <li>• Application form</li> <li>• Authority to screen</li> <li>• Written references including character/career checks</li> <li>• Public record check</li> <li>• Credit checks</li> <li>• Criminality checks</li> <li>• Proof of identity</li> </ul>	The relevant screening documents are stored on MyCheck for 6 months, then archived after a further 18 months for secure disposal. All documentation is retained in the personal file for seven years after employment has ceased.
<b>Care and Custody Only</b>	Detainee Records including: Detainee Property, Unit Diaries, Visitors logs, Incident reports, Security Intelligence Reports, Security records, Detainee Escort Risk Assessments and Detainee Core file, Local Operational and Security Audits plus Performance Records and other operational records.	7 years from date of last entry.
	Prisoner Escorting Records	Retained with detainee receiving authority, or 7 years after discharge.
	Assessment and Care in Detention Team ACDT records	Retained with detainee receiving authority, or 7 years after discharge.
<b>Care and Custody Health Only</b>	Patients' medical records and clinical notes including telephone advice records.	Electronic and paper records must be kept indefinitely, but where possible in accordance with NHS111.
<b>Whistleblowing cases (including fraud, bribery etc.)</b>	All records relating to each whistleblowing case for example, emails, investigation interviews & final reports, or any other supporting evidence	10 years after the date of closure of the case.
<b>Other</b>	Records and reports relating to technical matters and research	15 years after the requirements have ended.
	Donations granted	6 years.
	Deeds of covenant	6 years after the last payment made but up to 12 years if any payments are still outstanding or there is any dispute regarding the deed.

## Appendix

### Controls within this policy

Standard	Control Number	Description
ISO27001:2022	A 5.10	Acceptable use of Information Assets
	A 5.12	Classification of Information
	A 5.13	Labelling of Information
	A 5.14	Secure Transfer of Information
	A 5.33	Protection of Records
	A 5.34	Privacy and Protection of PII
	A 8.3	Information Deletion
	A 8.5	Data Leakage Prevention

### Definitions

### Exceptions

Any exception to this policy must be made via the security exception process, the decision of the Chief Information Security Officer is final.

### Support

This policy is maintained and reviewed on a regular basis by the Mitie Information Security team.



Phil Bentley  
Chief Executive Officer  
Mitie Group plc

17<sup>th</sup> March 2025