# Guidance 1.5: Considerations for Security Advisors

1. This guidance document provides a set of considerations for Security Advisors and Senior Security Advisors in relation to the Government Security Classification Policy on:

    - Roles and Responsibilities
    - Threat Model
    - Security Controls
    - Security Outcomes
    - Further Considerations
        i. Technology Capability
        ii. Personal Data and Risk Assessing Bulk Personal Data
        iii. Aggregation
        iv. Use of Protected Document Registry Books

## Roles and Responsibilities for Information Classification

2. One of the fundamental principles of the GSCP is that everyone who works for or with the government has a responsibility to safeguard any HMG information they handle (regardless of whether it is marked). This principle ensures everyone who handles HMG information is personally responsible and accountable for HMG information in their care. Although the onus is on the individual to correctly classify and appropriately handle information, there are other roles involved in the information classification process which provide advice and/or have responsibility in decision making.

3. This guidance acknowledges that some roles and responsibilities involved in setting the Government Security Classification Policy will remain fixed across all organisations (e.g. the Government Chief Security Officer), whilst others are recommended and may not necessarily align with all organisational structures e.g SSA/SAs. Each organisation should allocate and determine their equivalent roles in a pragmatic way that ensures sufficient strategic

oversight of: information risk management; organisational information security policy development and advice; and, information classification and handling.

## Defined roles for information classification

4. The roles that have a defined responsibility in setting baseline information security classification policy across government and all organisations, and advising on local implementation are:

   - **Government Chief Security Officer (GCSO)** - sets the GSCP baseline which organisations are mandated to follow and manages pan-government information security risks.

   - **Government Security Board (GSB) -** advises the GCSO on setting the GSCP baseline and pan-government risk.

   - **Government Security Group (GSG) Information Security Policy Team** - responsible for providing guidance to organisations on their classification policies (and decisions where necessary) and raising cases involving pan-government risks to the GCSO.

   - **UK National Security Authority (UK NSA)** - is the government authority with ultimate responsibility for the protection of classified information exchanged internationally. The UK NSA sits within the Government Security Group and sets overall protective security policy for international classified exchanges.

## Recommended responsibilities for information classification

5. The organisation should ensure that roles are defined within local policy and they at least cover the key responsibilities outlined in the suggested categories below, even if they are combined together or distributed across different roles.

   - **Governance:** responsible for setting and advising on information risk appetite and strategy;

     i. Setting the organisation's overall information security strategy and local risk appetite (e.g. Chief Executive, Permanent Secretary, Accounting Officer, Risk Boards).

     ii. Understanding an organisation's local information and cyber risk, and advising the Accounting Officer on what controls are necessary to protect the organisation's information assets and technologies (e.g. Chief Security Officer, Chief Information Security Officer, Chief Digital & Information Officer, Information Asset Owners).

- **Organisation's policy makers:** are responsible for advising on the development and implementation of organisational information security policy;

  i. Developing and maintaining departmental information security policies; incorporating changes based on cross-government policies; overseeing local information security policies and controls within business units; and, managing security incidents (e.g. SSA/SAs, Chief Security Officer).

  ii. Ensuring that the right policy, guidance, process and systems are in place so that information is stored and handled appropriately in accordance with its classification, and in line with best practice and any legislative or regulatory requirements (e.g. Knowledge & Information Management Manager, Data Protection Officer).

- **Operations:** responsible for the production, classification, handling, and disposal of information, and establishing escalation procedures for information classification decisions;

  i. Has authority over the production, classification, dissemination and disposal of an information asset (e.g. Information Creator).

  ii. Handling information proportionately and in line with HMG policy, and any applicable organisation's policies or contractual obligations (e.g. Information User, End User).

  iii. Ensuring staff are aware of their responsibilities for information classification, undertake the necessary training, understand their security requirements, and understand how legislation relates to their role, including potential sanctions (criminal or disciplinary) that may result from inappropriate behaviours (e.g Line Manager).

  iv. Establishing clear escalation and oversight procedures for managing information classification decisions that exceed local risk appetite and need to be considered outside the immediate team; and if needed, developing additional controls that exceed the baseline dependent on local risks (e.g. Deputy Director, Head of Business Unit, Accounting Officer).

## Threat model at OFFICIAL

6. Security classifications indicate the sensitivity of information AND the typical baseline behaviours and security controls necessary to defend HMG information against a broad profile of applicable threats. Risk owners should appreciate that information classified at one level cannot be assured to be protected against the threat profile associated with a higher level of classification.

7. The OFFICIAL tier provides for the generality of government business, public service delivery and commercial activity. This includes a diverse range of information, of varying sensitivities, and with differing consequences resulting from deliberate or unintended compromise or loss. OFFICIAL information must be secured against a threat model that is broadly similar to that faced by a large UK private company. The threat model for OFFICIAL classification tier anticipates a need to defend against a broad range of threat actors, which may include, but is not limited to: staff who pose insider risk, hacktivists, pressure groups, individual hackers, state actors and the majority of criminal individuals and groups.

8. This model does not imply that information within the OFFICIAL tier will not be targeted by some sophisticated and determined threat actors (including Foreign Intelligence Services) who may deploy advanced capabilities. It may be rather, a risk based decision has been taken not to invest in controls to assure protection against those threats, i.e. proportionate rather than guaranteed protection. Even whilst not seeking guaranteed protection, OFFICIAL can still be made a hard target through using proportionate risk-based decisions, to thwart threat actors that use well-known techniques, whilst also aiming to detect those using advanced capabilities.

9. Technical security controls at OFFICIAL will be based on assured, commercially available products and services, without need for any bespoke development. Whilst these controls cannot absolutely assure against the most sophisticated and determined threat actors, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access OFFICIAL information.

## Threat model at SECRET

10. The SECRET threat model anticipates a higher level of threat capability than would be typical for the threat model described in the OFFICIAL tier. The model includes, but is not limited to: capable state actors, some serious organised crime groups and staff who pose insider risk. Attacks may be bespoke in nature and tailored to specifically attack the target infrastructure. Vulnerable elements of the supply chain may be targeted to facilitate a further compromise of information.

11. Risk owners should appreciate that assured protection will not be provided against very sophisticated, persistent and blended attacks by the most capable and determined organisations (such as highly competent state actors). A level of risk acceptance is required - threat sources have the capability to successfully target information within this tier if they are motivated to do so.

## Threat model at TOP SECRET

12. The threat model at TOP SECRET reflects the highest level of capability deployed against the nation’s most sensitive information and services. Very little risk can be tolerated in this tier, although risk owners should note that no activity is entirely free from any risk.

## Security Controls for OFFICIAL, SECRET and TOP SECRET

The security controls outlined below consider a wide range of classified assets.  Specific or additional controls in place for individual assets (such as Rosa devices) will take precedence.

| | OFFICIAL | SECRET | TOP SECRET |
|---|---|---|---|
| **Personnel Security** | Minimum controls include:<br>● Appropriate recruitment checks (e.g. the BPSS, or equivalent)<br>● Reinforce personal responsibility and duty of care through training<br>● 'Need to Know' for sensitive assets | Additional minimum controls include:<br>● Always enforce Need to Know<br>● SC for regular, uncontrolled access<br>● Special Handling Instructions | Additional minimum controls include:<br>● DV for regular, uncontrolled access |
| **Physical Security**<br>a. Document handling | ● Clear desk / screen policy<br>● Consider proportionate measures to control and monitor access to more sensitive assets | ● Register and file documents in line with locally determined procedures<br>● Maintain appropriate audit trails<br>● Control use of photocopiers and multi-function digital | ● Register movement of documents and undertake annual musters<br>● Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and |

| | | | |
|---|---|---|---|
| | | devices in order to deter unauthorised copying or electronic transmission<br>● Limit knowledge of planned movements to those with a need to know | record results<br>● Strictly limit knowledge of planned movements to those with a need to know |
| b. Storage | ● Storage under single barrier and / or lock and key<br>● Consider use of appropriate physical security equipment / furniture (see the NPSA Catalogue of Security Equipment (CSE)) | ● Defence in Depth<br>● Use of NPSA Approved Security Furniture (refer to CSE)<br>● Segregation of shared cabinets<br>● Proportionate measures to control and monitor access / movements | ● Robust measures to control and monitor movements<br>● Information must be accountable |
| c. Remote Working | ● Ensure information cannot be inadvertently overlooked whilst being accessed remotely<br>● Store more sensitive assets under lock and | ● Risk assessment to determine need and identify appropriate protective security controls<br>● NPSA approved | ● Only to be removed for remote working as an exception if determined essential and following acceptance of the inherent risks by senior |

| | | | |
|---|---|---|---|
| | key at remote locations | security furniture at remote location (see CSE)<br>● Approval may need to be sought from the originator | management |
| d. Moving assets by hand | ● Single cover<br>● Precautions against overlooking when working in transit<br>● Authorisation required for significant volume of records/files | ● Risk assess the need for two people to escort the movement of document(s)/media<br>● Documented local management approval required and completion of document / media removal / movement register<br>● Sealed tamper-evident container / secure transportation products (refer to CSE)<br>● Not accessed in public areas | ● Senior Manager approval subject to risk assessment |

| | | | |
|---|---|---|---|
| e. Moving assets by post / courier | ● Include return address, never mark classification on envelope<br>● Consider double envelope for sensitive assets<br>● Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service | ● Local management approval required, actions recorded in document movement register<br>● Robust double cover<br>● Approved registered mail service commercial courier ('track and trace'), or government courier | ● Senior Manager approval subject to risk assessment<br>● Special handling arrangements may need to be considered |
| f. Moving assets overseas | ● Trusted hand under single cover<br>● Consider using reputable commercial courier's 'track and trace' service | ● Trusted hand (appropriate security clearance, e.g. SC/L2)<br>● Sealed tamper evident container / secure transportation products (refer to CSE)<br>● Where travelling to / via a country of 'Special Security Risk' the container should be | ● Security cleared (DV) diplomatically accredited courier only |

| | | | |
|---|---|---|---|
| | | carried by a diplomatically accredited courier | |
| g. Bulk Transfers | ● Local management approval, subject to departmental policy, appropriate risk assessment and movement plans | ● Senior management approval, subject to departmental policy, appropriate risk assessment and movement plans<br>● Commercial companies could be used provided information transported in sealed containers/ crates, accompanied by departmental staff and movement and contingency plans are in place | ● Local police aware of movement plan |
| **Electronic Information Security**<br>a. Electronic Information at Rest | ● Electronic Information shall be protected at rest in accordance with principles and guidance outlined in Cyber | ● Electronic Information will normally be protected at rest by physical security appropriate for | a. Electronic Information will normally be protected at rest by physical security appropriate for TOP |

| | | | |
|---|---|---|---|
| | Assessment Framework (CAF) B.3.<br>● End User Devices should be protected in line with the NCSC Device Security Collection for security principles and platform-specific guidance.<br>● Wherever data is stored, even temporarily, it may be vulnerable to unauthorised access, tampering or deletion. The NCSC's data security guidance will encourage activities for identifying what data you have and applying appropriate controls to mitigate identified data risks throughout its lifecycle. | SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with (revitalised) Enhanced Grade protection | SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with High Grade protection |

| | | | |
|---|---|---|---|
| b. Productivity/ Collaboration Suites | • Productivity/ Collaboration suites shall meet CAF principle B.2.<br>• Productivity/ Collaboration suites shall be configured to support cross-department working by default<br>• Productivity/ Collaboration suites shall be configured to make sharing information through official channels (sharing a link to a document) easier than sharing the same information in a different way (document attached to email)<br>• For cloud-based and cloud-enabled | • Should be provided by an appropriate organisation with an ongoing accreditation/ assurance function<br>• Where available, sensitivity controls should be enabled<br>• Generally storage will be local rather than cloud-provided | c. On segregated networks with appropriate cross-domain solutions enabled at the edges |

|  |  |  |  |
|---|---|---|---|
|  | products, you should follow the NCSC Cloud security guidance<br>- For Microsoft 365 / Microsoft Office 365, you should follow: NCSC Securing Office 365 guide and the Microsoft 365 Collaboration Blueprint for UK Government |  |  |
| d. Electronic information in transit. (Email) | - Electronic Information in transit shall be protected at rest in accordance with CAF B.3.<br>- Information may be emailed / shared to external partners / citizens, subject to local business policies and procedures<br>- You shall implement policy on Securing | - Well-configured Cross Domain Solutions will be used to manage all ingress and egress of electronic information.<br>- Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) | - Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption<br>- Information will only be shared with specific users or groups with robust identity |

| | | | |
|---|---|---|---|
| | Government Email including supporting at minimum Transport Layer Security Version 1.2 (TLS v1.2) or an updated TLS Version for sending and receiving email securely.<br>● To protect email systems and ensure the confidentiality and integrity of government data, departments shall have Domain-based Message Authentication Reporting and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domains. This | Enhanced Grade encryption<br>● Information will only be shared with specific users or groups with robust identity verification in place on recipient ICT systems | verification in place on recipient ICT systems |

| | | | |
|---|---|---|---|
| | shall be accompanied by the use of Mail Transfer Agent Strict Transport Security (MTA-STS) and TLS Reporting (TLS-RPT). Spam and malware filtering controls shall also be implemented on inbound email | | |
| e. ICT services | - ICT services should identify, assess and understand security risks in accordance with CAF A.2<br>- ICT services could be designed in alignment with Secure By Design principles<br>- ICT services could follow the NCSC device security guidance as applicable based on | - ICT Services must be accredited as appropriate considering the SECRET threat model. NCSC design patterns or bespoke advice may be required<br>- Very careful risk assessment and understanding of implications of enabling functionality<br>- Information exchange | - ICT systems designed must be accredited as appropriate considering the TOP SECRET threat model. Bespoke architectural advice may be necessary |

| | | | |
|---|---|---|---|
| | ICT architectural approaches and risk management processes<br>- ICT services developed by a Department or delivery partner must follow the risk management processes as set out in NCSC Risk Management Toolbox and follow standard architectural approaches | outside of the SECRET tier will be highly constrained and managed using shared accredited capability | |
| f. Removable Media (data bearing) | - The use of removable media should be minimised, and other approved information exchange mechanisms should be used where available in preference to removable media<br>- Any information moved | - Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection | - Content must be appropriately encrypted unless (by exception) there exists appropriate full life physical protection |

| | | | |
|---|---|---|---|
| | to or transferred by removable media shall be minimised to the extent required to support the business requirement<br>● Consider appropriate encryption to protect the content, particularly where it is outside the organisation’s physical control | | |
| g. Telephony (Mobile and Landline) | ● Details of sensitive material should be kept to a minimum<br>● Recipients should be waiting to receive faxes containing personal data and / or data marked – SENSITIVE | ● Secure Telephony, VTC and secure fax | ● Secure Telephony, VTC and secure fax |
| **Archiving and Transfer to The National Archives** | ● Transfer as open records wherever possible, at 20 years | ● Retain as long as classification level applies | ● Retain as long as classification level applies |

| | | | |
|---|---|---|---|
| | and in accordance with the Public Records Act | | |
| **Disposal / Destruction**<br>*Guidance about the physical destruction of assets is available within the NPSA's Secure Destruction guidance (February 2023).*<br>*Electronic media used to process HMG assets must be sanitised and disposed of in accordance with the requirements in NCSC's Secure Sanitisation of Storage Media* | ● Dispose of with care using approved commercial disposal products to make reconstitution unlikely (refer to NPSA guidance and NCSC's Secure Sanitisation of Storage Media) | ● Verify document is complete before destruction<br>● Use approved equipment and or service providers listed in the CSE | ● Control measures to witness / record destruction |
| **Incident Reporting**<br>*Guidance about the management and handling of security incidents is available in the GOV007 Functional* | ● Local reporting arrangements<br>● Escalation to DSO and SSA/SA as appropriate for significant incidents<br>● ICO notified of | ● DSO and SSA/SA notified, local procedures followed<br>● Consider notifying Accounting Officer and responsible Minister | ● Accounting Officer, Minister and Cabinet Office alerted |

|  |  |  |  |
|---|---|---|---|
| *Standard.*<br>*Relevant ICO guidance should also be consulted.* | “significant” losses of personal data<br>● GSG and NCSC for ICT incidents | ● ICO notified if personal information<br>● May be appropriate for police investigation subject to damage test and Cabinet Office gateway process |  |

## Security Outcomes

13. To defend against the threats outlined in the threat model, the security controls outlined above should achieve the following outcomes at each classification tier:

| | OFFICIAL | SECRET | TOP SECRET |
|---|---|---|---|
| Outcome | ● Meet legal and regulatory requirements<br>● Promote responsible sharing and discretion<br>● Proportionate security behaviours appropriate to an asset's sensitivity<br>● Make accidental compromise or damage unlikely | ● Make accidental compromise or damage highly unlikely<br>● Detect and resist deliberate attempts at compromise<br>● Make it highly likely those responsible will be identified | ● Prevent unauthorised access<br>● Detect actual or attempted compromise<br>● Identify those responsible and respond appropriately |
| Personnel Security | ● Access by authorised individuals for legitimate business reasons on a need-to-know and share basis. | ● Assurance that access is only by known and trusted individuals | ● High assurance that access is strictly limited to known and trusted individuals |
| Physical Security (handling, use, storage, | ● Proportionate good practice precautions against accidental or opportunistic compromise | ● Detect and resist deliberate compromise by forced and surreptitious attack<br>● Destroy / sanitise to make | ● Robust measures to prevent compromise by a sustained and sophisticated or violent attack<br>● Destroy / sanitise to prevent |

| | | | |
|---|---|---|---|
| transport and disposal) | ● Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely | reconstitution and / or identification of constituent parts highly unlikely | retrieval and reconstitution |
| Electronic Information | ● Protect against deliberate compromise by automated or opportunist attack<br>● Aim to detect actual or attempted compromise and respond. | ● Detect and resist deliberate compromise by a sophisticated, determined and well resourced threat actors | ● Robust measures to prevent compromise from sustained attack by sophisticated, determined and well resourced threat actors |

## Further Considerations

## Technology Capability

14. Where available and proportional to implement, organisations could apply modern technology and security tactics, in a user-centric way, to assist personnel with their responsibilities to manage HMG information well. For example, the use of technology to encrypt and decrypt data automatically, so as to remove the number of steps required for personnel to complete their legitimate work tasks; or, the use of technology to prompt users automatically of the potential security risks of how they are sharing a document.

15. Organisations should identify information they hold that is at the higher-end of the OFFICIAL classification range (for example, where its intentional or unintended compromise could lead to a threat to life), and consider whether additional measures to protect the information should be applied above the organisation's baseline for OFFICIAL and/or OFFICIAL information marked "-SENSITIVE". Organisations should consider the use of collaborative IT systems with additional security controls (such as Rosa) for storing, processing and sharing of particularly sensitive data sets.

16. SA/SSAs could also engage with IT teams to deploy information labelling tools to aid classifying information and applying additional markings to information. Any information labelling tools implemented to comply with the GSCP should meet accessibility requirements and be compatible with screen readers and assistive technology. Further guidance is available from GSG and the Cabinet Office.

17. The use of technical capabilities to provide additional controls are recommended but not mandatory where adequate procedural and personnel controls are in place to ensure that the stated policy outcomes for labelling, classification and protection of data are in place. Technology capability should complement existing controls.

## Personal Data

18. The Data Protection Act 2018 and UK GDPR underpins how organisations, business and government, must protect citizens' personal data by law. Organisations which process citizens' personal data have a responsibility to protect that data proportionately in accordance with the 'data protection

principles'. Organisations should take particular care when processing special category data, ensuring that any security controls or alternative risk management measures applied to it are commensurate with the risks of compromise associated with that information.

19. There should be timely consultation of local data protection leads where further guidance is required on appropriate measures to protect personal data. In planning for and during crisis events, this should include: preparations in advance (such as data sharing agreements); proportionate, temporary data arrangements during a crisis event; and, the standardisation of temporary arrangements (returning to a business as usual state) post-crisis.

20. Organisations should have procedures in place to triage information requests. Triage procedures should identify those requests involving the potential disclosure of personal data and ensure that any necessary additional controls on that data are applied. Triage processes should include the removal of any personal data that is not intended for release prior to disclosure, including hidden data. Further information on publishing information safely and identifying hidden data can be found on the ICO website.

## Risk assessing bulk personal data

21. The NCSC's Data Handling principles provide a set of good practices for the secure storage and handling of sensitive personal data, including Special Category Data. These principles are not, however, a replacement for a comprehensive risk management strategy for protecting personal data in an organisation.

## Data Aggregation

22. Data aggregation is the combining of a number of data points. Aggregation can be performed in one data set or by combining data from different data sets, and can occur through accumulation (by volume) or through association/links. Aggregation can be beneficial to organisations and is often necessary for developing insightful statistical analysis.

## Aggregation: risk management

23. Data controllers should be mindful of any data protection issues that may arise from aggregating data. For example, aggregating data from separate sources (especially sensitive information and personal data) could lead to the unintentional identification of individuals, even where no specific personal data is present. Further advice on data protection considerations can be sought from local legal advisers and data protection leads.

24. Data controllers should also be aware of the potential value of aggregated information to threat actors, as relationships created between data points in a combined dataset - although unintended - can make aggregated information more useful than the sum of its parts. If compromised, aggregated data can be used by threat actors to gather latent intelligence[1], generate finances through ransom or resale on the black market, or significantly hamper government operations by withholding, manipulating or damaging the data.

25. Security controls and/or risk management measures should be in place to protect aggregations of personal data, including unintended use and disclosures. These controls should be commensurate with the size and sensitivity of the data, as well as the risk of harm posed to individuals whose data is being processed. A data protection impact assessment should be carried out prior to the introduction of any system that involves the regular processing of personal data on a large scale.

## Aggregation and classification

26. Aggregating data will not usually affect the classification of the component information, but a new piece of data or set of data, formed as a result of associations, may need to be classified at a higher level. The context should be assessed by an organisation, especially where further associations are enabled through the aggregation of mixed data sets, which might increase the classification of that data aggregation, possibly resulting in an increased interest from threat actors with advanced capabilities. Where an increase in classification is, or is not, required, there may also be some additional protective measures, above the classification related protections for the component information, that are justified to manage the additional risks of bulk aggregation. If aggregated data contains information with a range of classifications, a suitable system must be marked with at least the highest classification level contained in the component data (e.g. Rosa could be considered a suitable system at SECRET).

27. Users can apply additional markings, or stronger technical controls above the central or organisational baselines for the relevant classification tier to protect aggregated information. In some circumstances, it may be necessary to protect sensitive sub-sets of the aggregated dataset, by appropriate processing being carried out on higher-tier IT systems. It should not usually

[1] Latent intelligence' has been termed to describe consequential, and sometimes completely unintended, information that can be determined arising from the complexities of large amounts of data.

be necessary to give the dataset, as a whole, a higher classification than its component parts, allowing appropriate sharing of each part of the aggregated data at the appropriate classification. Users should check with their organisation's security team if they are unsure about how to proportionately protect an aggregated dataset in a given case.

## Keeping a Protected Document Registry Book

28. HMG organisations must keep a protected document registry book (PDR) when storing and handling hard copies of information assets that are classified at SECRET and TOP SECRET.[2]

29. It is at the discretion of the organisation's security team to decide whether to keep the sample PDR template (PDF format) provided as a hardcopy or to create their own digital version of the PDR using the same standardised fields included in the template. Organisations may add additional mandatory fields to the form to meet local requirements.

30. At a minimum, the PDR form should detail: who the information or data asset has been accessed by; if any transfers have taken place; when the information or data asset was returned; and, the date the document was destroyed.

31. The PDR should be appropriately protected and controlled. When a PDR is stored digitally, its access should be restricted to just those in charge of managing it. Those managing the PDR should hold the necessary security clearance to access the document.

32. If an electronic PDR is used, it should only be stored on a shared drive where access and editing can be restricted to the registration officer, their deputy and the minimum number of IT administrators. Consideration should be given on whether to store the electronic logbook on a SECRET level system (e.g. Rosa) rather than the OFFICIAL IT system, but this is not mandatory and therefore a decision that should be taken locally by the SA/SSA.

33. A SECRET or TOP SECRET hardcopy document must be registered on the PDR. By exception, and if permitted locally by the SSA/SA, hardcopy documents need not be registered in a PDR if they are working documents and destroyed within five days of being printed.

[2] A PDR template is available to HMG organisations upon request at: GovernmentSecurity@cabinetoffice.gov.uk

34. Local organisational policy set by an SSA/SA should determine how long a PDR should be retained after all the information held within it has been destroyed.

# Version History

| Document Version | Date Published | Summary of Changes |
|---|---|---|
| 1.0 | 30 June 2023 | ● First version published on GOV.UK |
| 2.0 | 5 August 2024 | ● Summary of August 2024 update:<br>○ New text prefacing the table on Security Controls for OFFICIAL, SECRET and TOP SECRET<br>○ New paragraph in Further Considerations - Technology Capability on considerations around information within the OFFICIAL tier.<br>○ Further Considerations - Personal Data section updated.<br>○ Guidance on Data Aggregation, Aggregation: Risk Management and Aggregation and Classification updated. |