Digital Directorate
(iTECS) Information and Technology Services Division
Cyber Security and Defence

The Scottish Government

Scottish Government
Data Handling Standard

Information Assurance & Risk
August 2018

Document Control

Date	Version	Name	Role	Reason For Change
14/08/2018	0.1	Jeremy Winchester	Author	First draft
03/09/2018	0.2	Jeremy Winchester	Author	Updated following CS&D comments/suggestions
03/09/2018	0.3	Jeremy Winchester	Author	Updated following CS&D comments/suggestions
04/09/2018	1.0	Mark McKenny	Document Approver	Approved Document
06/08/2019	1.1	Richard Birkett	Author	Minor amendments - reflect SBC advice re paper disposal arrangements
23/9/2019	1.2	Richard Birkett	Author	Minor amendments to reflect SBC advice in document handling section

Background

1. This document describes personnel, physical and information security controls which need to be applied when working with Scottish Government (SG) assets.

2. The controls are cumulative: minimum measures for each classification provide the baseline for higher levels. Personnel, physical and information security controls are based on commercial good practice, with an emphasis on staff to respect the confidentiality of all information.

3. Staff may need to apply additional controls over the baseline controls to manage specific risks to particular types of information. Such exceptions must be agreed with the respective Information Asset Owner.

4. This guidance is complemented by completing the “Responsible for Information (2018)” e-learning course, available from Civil Service Learning.

5. The following table describes the baseline control measures required when working with SG information assets. More stringent controls may be appropriate to manage more sensitive assets.

1. Data Handling Standard

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Personnel Security	• Appropriate recruitment checks (e.g. the BPSS, or equivalent) • Reinforce personal responsibility and duty of care through training • 'Need to know' for OFFICIAL-SENSITIVE assets	• Always enforce Need to Know • Security Cleared for regular, uncontrolled access • Special Handling Instructions apply	• DV for regular, uncontrolled access
Physical Security			
Document Handling	• User must lock their computing devices screens when leaving them unattended • All documents classified as OFFICIAL or OFFICIAL-SENSITIVE, must be securely locked away when not in use	• Register and file documents in line with SG determined procedures • Maintain appropriate audit trails • Control use of photocopiers and multi-function digital devices in order to deter unauthorised copying or electronic transmission • Limit knowledge of planned movements to those with a need to know	• Register movement of documents and undertake annual musters • Conduct random spot checks of documents to ensure appropriate processing / handling / record keeping and record results • Strictly limit knowledge of planned movements to those with a need to know

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Storage	• Storage under single barrier and / or lock and key • Consider use of appropriate physical security equipment / furniture (see the CPNI 'Catalogue of Security Equipment', CSE)	• Defence in Depth approach • Use of CPNI Approved Security Furniture (refer to CSE) • Segregation of shared cabinets • Proportionate measures to control and monitor access / movements	• Robust measures to control and monitor movements • Information must be accountable
Remote Working	• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Mobile systems, devices or information must never be left unattended unless shut down and physically locked down, locked away or otherwise secured	• Risk assessment to determine need and identify appropriate protective security controls • CPNI approved security furniture at remote location (see CSE) • Approval may need to be sought from the originator	• Only to be removed for remote working as an exception if determined essential and following acceptance of the inherent risks by senior management

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Moving assets by hand	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files	• Risk assess the need for two people to escort the movement of document(s)/media • Documented SG management approval required and completion of document / media removal / movement register • Sealed tamper-evident container / secure transportation products (refer to CSE) • Not accessed in public areas	• Senior Manager approval subject to risk assessment
Moving assets by post / courier	• Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service	• SG Management approval required, actions recorded in document movement register • Robust double cover • Approved registered mail service commercial courier ('track and trace'), or Government courier	• Senior Manager approval subject to risk assessment • Special handling arrangements may need to be considered

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Travelling Overseas (Moving assets by hand) – In addition to *Moving assets by hand* security controls	• Information taken overseas must be limited to the minimum required • The Security and Business Continuity team and the Cyber Security and Defence team must be notified • Authorisation to travel required subject to risk assessment • Trusted hand under single cover	• Senior Manager approval subject to risk assessment • Trusted hand (appropriate security clearance, e.g. SC)	• Senior Manager approval subject to risk assessment
Moving assets overseas (by post)	• Consider using reputable commercial courier's 'track and trace' service	• Sealed tamper evident container / secure transportation products (refer to CSE) • Where travelling to / via a country to which special security regulations apply the container should be carried by a diplomatically accredited courier	• Security cleared (DV) diplomatically accredited courier only

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Bulk Transfers	• Requires the approval of the Information Asset Owner, appropriate risk assessment and movement plans	• Senior management approval, subject to departmental policy, appropriate risk assessment and movement plans • Commercial companies can 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
Information Security			
Electronic information at rest	• Electronic Information will be protected at rest by default. This may be appropriate physical protection (such as data at rest in a government data centre) or may involve Foundation Grade data at rest encryption when physical control isn't guaranteed (such as on a laptop)	• Electronic Information will normally be protected at rest by physical security appropriate for SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with (revitalised) Enhanced Grade protection	• Electronic Information will normally be protected at rest by physical security appropriate for TOP SECRET assets. Where data is at rest on non-physically secure devices it will be encrypted with High Grade protection

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Electronic information in transit	• Information in transit between Government or other trusted organisations will be via accredited shared infrastructure (such as PSN) or protected using Foundation Grade encryption • Where more sensitive information must be shared with external partners (e.g. citizens), consider using secure mechanisms (e.g. browser sessions using SSL / TLS)	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or (revitalised) Enhanced Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems	• Electronic information will only be exchanged via appropriately secured mechanisms. This will involve use of appropriately accredited shared services or High Grade encryption • Information will only be shared with defined users on appropriate and accredited recipient ICT systems
Email	• OFFICIAL information may be sent in the clear over the internet • OFFICIAL-SENSITIVE information should be encrypted on the basis of risk	• Not permitted on SCOTS. Please contact the Office of Protective Security to discuss	• Not permitted on SCOTS. Please contact the Office of Protective Security to discuss

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
ICT Services	• Different GCloud services will be suitable for different types of OFFICIAL information. Risk owners MUST read and understand any GCloud accreditation residual risk statements • ICT services developed by the SG or delivery partner must follow risk management and follow standard architectural approaches • End user devices will conform to the security principles defined in the End User Device (EUD) Strategy: Security Framework and Controls	• SCOTS must not be used to store or process SECRET information • ICT Services must be protected as appropriate considering the SECRET threat model. NCSC design patterns or bespoke advice may be required • Very careful risk assessment and understanding of implications of enabling functionality • Information exchange outside of the SECRET tier must be highly constrained and managed using shared accredited capability	• SCOTS must not be used to store or process TOP-SECRET information • ICT systems designed must be accredited as appropriate considering the TOP SECRET threat model. Bespoke architectural advice may be necessary

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Removable media	• The use of removable media will be minimised, and other approved information exchange mechanisms should be used where available in preference • Any information moved to or transferred by removable media must be minimised to the extent required to support the business requirement • Consider appropriate encryption to protect the content, particularly where it is outside the organisation's physical control	• 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

	Official	Secret	Top Secret
Telephony	**Minimum controls include:**	**Additional minimum controls include:**	**Additional minimum controls include:**
	• Details of sensitive material should be kept to a minimum • Recipients should be waiting to receive faxes containing personal data and / or data marked with the OFFICIAL – SENSITIVE caveat • Sensitive conversations or those involving OFFICIAL SENSITIVE information must not be carried out in public	• Secure Telephony, VTC and secure fax	• Secure Telephony, VTC and secure fax

	Official	Secret	Top Secret
	Minimum controls include:	**Additional minimum controls include:**	**Additional minimum controls include:**
Disclosure			
	• Much of the information in this domain is likely to be releasable unless an FOI exemption is in force, it is personal data subject to Data Protection / GDPR legislation or there is another statutory bar • Official Secrets Act (OSA) and criminal cases subject to damage tests. • Where appropriate, non-sensitive information should be published for reuse	• Likely to engage FOIA exemption in whole or in part (e.g. 23, 24, 26, 27, 31), to be assessed on a case by case basis ● Some information might be releasable in a securely redacted format	• Subject to a case by case assessment there is a general presumption that information is: ○ above the OSA Prosecution threshold ○ subject to FOIA exemptions on National Security (or other) grounds
Archiving and Transfer to The National Records of Scotland			
	• Transfer as open records wherever possible, at 20 years and in accordance with the Public Records (Scotland) Act 2011	• Retain as long as classification level applies	• Retain as long as classification level applies

	Official	Secret	Top Secret
Disposal / Destruction	**Minimum controls include:**	**Additional minimum controls include:**	**Additional minimum controls include:**
	OFFICIAL: • Documents can be recycled if they do not have a handling instruction that limits circulation in any way. They can also be disposed of using an approved shredder. **OFFICIAL-SENSITIVE:** • Dispose of Official — Sensitive documents using an approved shredder. • Bulk shredding of OFFICIAL documents can be arranged via the SG contract (confidential waste bags); these can be collected by calling Help Central and should be stored securely until such time as they are uplifted; contact Security and Business Continuity (via our operations mailbox: Opsec@gov.scot) for advice.	• Verify document is complete before destruction • Use approved equipment and or service providers listed in the CSE	• Control measures to witness / record destruction • All shredding must be witnessed by another member of staff. • Keep the waste secure. • Record the destruction of the document in the Document Register, including two signatures (the person doing the destruction and a witness)

	Official	Secret	Top Secret
Incident Reporting	**Minimum controls include:**	**Additional minimum controls include:**	**Additional minimum controls include:**
	• To report an incident, colleagues should use the security incident reporting tool • Any loss, theft, misplacement or unauthorised access of systems, devices or information must be reported immediately using the cyber security hotline (0131 244 5111) or to the security control room (0131 244 5203) when outside of normal working hours • Escalation to Head of Security and SIRO as appropriate for significant incidents • ICO notified of losses of personal data	• Head of Security and SIRO notified • Consider notifying Accounting Officer and responsible Minister • ICO notified if personal information • May be appropriate for Police investigation subject to damage test and Cabinet Office gateway process	• Accounting Officer, Minister and Cabinet Office alerted