

PROTECTING GOVERNMENT INFORMATION · GUIDE 5 OF 6

Information security

Marking and sending OFFICIAL-SENSITIVE information, and the desktops, laptops, tablets and phones that hold it.

WHERE THE REQUIREMENTS COME FROM

The information itself

Information security is about the government material you hold: knowing what it is, where it lives, who can reach it and how it moves. Most of the specific rules a supplier meets sit in this area.

Source	What it asks for
Government Security Classifications Policy Version 2.0, with Guidance 1.1, 1.4 and 1.6	What OFFICIAL and OFFICIAL-SENSITIVE mean and how material is marked and handled. Contractors handle government information in line with the policy.
Central government contracts Security schedule and UK GDPR	The handling and transfer rules set in the schedule and your Security Management Plan. Where personal data is involved, the security duties of the UK GDPR apply as well.
MOD contracts Security Aspects Letter, DEFCON 660 and the Contractual Security Conditions	What is sensitive on the contract, and the conditions for storing, sending, encrypting and destroying it, currently Annex B to Industry Security Notice 2026/04.
MOD topic notices Industry Security Notices	Specific rules on remote working (2022/10), email and file transfer (2023/04), cloud services (2024/06) and incident reporting (2025/03).

A companion document, the Secure Endpoint Framework for Government Suppliers, sets out a full device and service baseline with the evidence each control should produce. This guide gives the principles. The framework gives the detail.

KNOWING WHAT YOU HOLD

Marking, ownership and a register

The Classifications Policy's Quick Read says OFFICIAL-SENSITIVE is not a separate classification tier. It is OFFICIAL information carrying a marking, handled on the same kind of systems with tighter behaviour from the people using it and any extra conditions your customer sets.

Know what the customer has given you

For MOD work, the Security Aspects Letter says which parts of the contract are OFFICIAL-SENSITIVE, and you return a signed acknowledgement before work begins. For central government work, the security schedule sets the category of data and the controls that go with it. Either way, read it before the first file arrives.

Name an owner and keep a register

Government departments give each information asset a named owner. A supplier can follow the same principle for its own copy of a customer's information: one senior person, usually a director, who decides who may access it and signs off its disposal. Keep one register entry per contract, recording what is held, where, who may reach it and what happens to it at the end.

Mark what you create

Documents you produce from OFFICIAL-SENSITIVE material carry the same marking, in the header and footer, as Guidance 1.1 of the Classifications Policy describes.

Watch aggregation

A collection of individually unremarkable information can be more sensitive than any single item in it. A full set of drawings for a site, or a spreadsheet of staff and locations, may need more care than the separate files did. Keep only what the work needs and remove working copies when the task is done.

DEVICES

Desktops, laptops, tablets and phones

"Don't look for assurance that a system is 'good for OFFICIAL-SENSITIVE'."

Cabinet Office and Government Digital Service, 'OFFICIAL-SENSITIVE' data and IT, last updated February 2017

No device or product is certified for OFFICIAL-SENSITIVE. What a supplier can do is hold every device that reaches government information to one written standard, and show that it stays there.

Company owned and centrally managed

Guidance 1.1 of the Classifications Policy says handling significant OFFICIAL-SENSITIVE information on a privately managed device through non-corporate channels can only be justified in exceptional circumstances. For MOD work, Industry Security Notice 2022/10 requires company issued and managed devices within the UK, and personal devices and accounts are not to be used.

Control	What good looks like
Encryption	Every device encrypted with the platform's built-in encryption. The MOD conditions require it for any portable device holding OFFICIAL-SENSITIVE information.
Sign-in	A PIN or biometric unlock on the device, and multi-factor authentication on every cloud service.
Screen lock	Locks after no more than 15 minutes, which is the MOD figure. Phones and tablets should lock sooner.
Updates and protection	Automatic updates, with high-risk updates applied within 14 days, and malware protection running.
Administration	Users work without administrator rights, and devices that fall out of line lose access to government information until fixed.
Removable media	USB storage blocked by default, with encrypted company media allowed only where a need is approved.

STORING AND SENDING

Where information lives and how it moves

Where it may be held

- **In your organisation's own services.** A company tenant or file store named in the register, never a personal email account or personal cloud storage.
- **In cloud services you have checked.** For MOD work, Industry Security Notice 2024/06 requires services holding MOD information to align with the National Cyber Security Centre Cloud Security Principles, reviewed at least yearly. For central government work, follow the schedule.
- **In the UK.** MOD work is done within the UK. For any government customer, information goes abroad only with the customer's prior agreement.
- **On devices only as long as needed.** Local copies kept to a minimum and removed when the work is done.

How it may move

Situation	Rule
Email at OFFICIAL	May be sent over the internet without additional encryption.
Email at OFFICIAL-SENSITIVE	For MOD work, sent encrypted using an approved technique such as TLS at version 1.2 or higher. Central government schedules set their own rule.
Encrypted files	For MOD work, a password of at least nine characters, sent by a separate route.
Personal accounts	OFFICIAL-SENSITIVE information is never sent to a personal device or personal account.
Subcontractors	Shared only where the contract and the register allow it, and after the subcontractor has accepted equivalent conditions.
Printing	Kept to a minimum, and never on a public or personal printer.

WHEN THINGS GO WRONG, AND AT THE END

Incidents, lost devices and disposal

Reporting

For MOD work, the conditions say a loss or compromise is reported to the customer immediately, and Industry Security Notice 2025/03 makes the Defence Industry WARP the point of report for every security incident affecting defence related classified material. The notice sets the latest times: no later than 72 hours for OFFICIAL-SENSITIVE and five working days for OFFICIAL. Report a lost device as soon as you know.

For central government work, follow the route in the security schedule, normally to the contract manager. Where personal data is involved and you act for the department as a processor, the UK GDPR requires you to tell the department without undue delay.

A lost or stolen device

- 1 Report it at once**
To the owner of the information inside your organisation, and then by the contractual route.
- 2 Lock and wipe it remotely**
Revoke the user's sessions and sign-in tokens at the same time.
- 3 Record what it could reach**
Which information, and whether the device was encrypted and compliant when it last checked in.
- 4 Learn from it**
Review the cause and change the arrangements if they need changing.

Disposal and the end of a contract

National Cyber Security Centre guidance treats a factory reset of an encrypted device as proportionate for OFFICIAL data. The MOD conditions add the use of an erasure product. For devices that have held MOD information, do both, or use a destruction provider that issues a certificate. At the end of a contract, return or destroy the customer's information as they direct, and record which was done.

EVIDENCE

What this area should produce

Record	What it shows
Signed Security Aspects Letter acknowledgements, or the contract schedule	What each customer requires
The register of government information held	What is held, where, and who owns it
A written device standard with its approval date	The baseline every device is held to
A current device compliance report	That each device meets the standard today
Incident and loss log	That reports were made, and in time
Disposal and return records	What happened to information at the end

Where this area meets the others

Information security is where the other areas meet in practice. Every rule in this guide depends on the others working as well, which is why Guide 6 shows how to hold all four together as one set of arrangements.

HOW THE MARK LOOKS AT THIS AREA

Under the Westmark Defence Supplier Mark, information handling is examined at every scope, from marking and storage through to return and destruction. Leaving a known exposure of controlled information unaddressed, or failing to report a loss, prevents a positive outcome.

WESTMARK ASSURANCE

Where the Defence Supplier Mark fits

Westmark Assurance provides independent security assurance, assessing organisations, premises and security arrangements against defined standards and frameworks.

The Westmark Defence Supplier Mark is for companies that supply defence and government. It assesses how an organisation identifies, controls and evidences security risk across the work it delivers, against a published standard and control set. The criteria are published in full at westmarkassurance.co.uk, so you can read exactly what is examined before you decide anything.

If you would like help putting these arrangements in place, we can introduce you to a Licensed Partner. Their preparation work is kept separate from our assessment, so an organisation they have supported is always assessed by someone independent of them.

Talk to us

For a conversation about the Defence Supplier Mark, or an introduction to a Licensed Partner:

hello@westmarkassurance.co.uk · 033 33 356 873

1st Floor, 2 West Regent Street, Glasgow, G2 1RW

Westmark Assurance is not an accredited certification body and does not offer UKAS-style certification. An outcome is a judgement by Westmark Assurance and carries no certification, accreditation or approval by government or the Ministry of Defence.

Westmark Assurance is a trading name of Ross Macdonald Consultancy Ltd, registered in Scotland, number SC848204. Registered office 1st Floor, 2 West Regent Street, Glasgow, G2 1RW.