

PROTECTING GOVERNMENT INFORMATION · GUIDE 2 OF 6

Physical security

What the contract conditions ask of a supplier's premises and people, from storing government material to working on a customer's site.

WHERE THE REQUIREMENTS COME FROM

What physical security has to do for a supplier

Physical security keeps government material out of the hands of people who should not have it, at your own premises, in transit, at home and on your customer's sites. The rules are short and practical, and most of them apply to organisations of every size.

Source	What it asks for
Government Security Classifications Policy Guidance 1.1 and 1.4	OFFICIAL-SENSITIVE material kept "under lock and key when unattended" and a clear desk. Home working is protected to the same standard as the office. It applies to contractors as well as civil servants.
Central government contracts Security schedule	The physical controls the buyer expects, recorded in your Security Management Plan. Where the schedule is silent, the Classifications Policy behaviours still apply.
MOD contracts Contractual Security Conditions, Annex B to Industry Security Notice 2026/04	Material physically secured against unauthorised access, access limited to those with a need to know, devices never left unattended in public or in a vehicle, destruction to a set standard and immediate reporting of any loss.
Work at MOD establishments DEFCON 76 and site regulations	The establishment's own security regulations, which apply to your people for as long as they are on site.
National Security Act 2023 Industry Security Notice 2024/03	Supplier land and buildings used for defence purposes in support of UK forces' weapons, equipment or capabilities are prohibited places. Signage is recommended, and unauthorised approach or entry can be an offence.

Facility Security Clearance, formerly List X, applies to suppliers holding material at SECRET and above. Work at OFFICIAL-SENSITIVE does not need it, and the conditions ask for lockable storage. Rated security containers are needed only where your customer specifies them.

YOUR OWN PREMISES

Storage, access and a clear desk

The MOD conditions state the storage requirement in a single sentence: OFFICIAL-SENSITIVE material "shall be stored under lock and key and shall be placed in a lockable room, cabinets, drawers or safe and the keys/combinations shall be controlled".

What that looks like in practice

- **A known place for each holding.** Record where each customer's paper and removable media are kept, so anyone checking can find them and see who has access.
- **Key and combination control.** A short list of named keyholders, with combinations changed whenever someone who knows them leaves.
- **Access on need to know.** Material is available to the people working on that contract, and a cabinet shared with the rest of the office is only suitable where everyone with the key has that need.
- **A clear desk.** Guidance 1.1 of the Classifications Policy says: "Keep your desk clear of hard copy information not in use." Papers go back in the cabinet at the end of the day and whenever the desk is left.
- **Screens and printers.** Screens are positioned so visitors cannot read them, and printing is collected straight away from a printer inside the office.
- **Visitors.** Visitors are signed in and accompanied wherever government material is in use. None of the published conditions states this, and it is what a customer's security team will expect to see.

Proportionate for a small business

A two-person practice can meet all of this with a lockable filing cabinet in a lockable office and a written note of who holds the keys. The outcome matters more than the equipment. A larger firm will usually need a controlled room with a key register, checked regularly.

AWAY FROM YOUR PREMISES

Working from home, travelling and carrying material

Guidance 1.4 of the Classifications Policy expects information to be protected to the same standard when working remotely as in the office. Away from the office there is no locked room to fall back on, so the rules need to be clear to everyone who carries material.

Situation	What to do
Working at home	Work where you cannot be overlooked, keep paper to a minimum and lock it away when you step away. Nothing is printed on a home or personal printer.
In a vehicle	The MOD conditions say portable devices holding the customer's data "are not to be left unattended in any motor vehicles". The same applies to paper. Take it with you.
On public transport and in public places	No reading OFFICIAL-SENSITIVE material where others can see it, a privacy screen on laptops, and calls about the work taken somewhere private. Devices are never left unattended in a public place.
Carrying papers or media	Only what the task needs, kept on your person or in a closed bag that stays with you. Sign-in tokens and PINs are kept apart from the device.
Overseas	MOD work is done within the UK. Taking government information abroad needs the customer's prior agreement.

Your security procedure should say which of these apply to your organisation, and your staff briefing should cover them in plain terms. Guide 3 covers the briefing, and Guide 5 covers the devices themselves.

ON GOVERNMENT SITES

When your people work at a customer's establishment

Survey, inspection, maintenance and construction work often takes a supplier's staff onto MOD and other government sites. DEFCON 76 governs that work for the MOD, and the establishment's own regulations apply alongside it. Where the site's rules and your own differ, the site's rules take precedence.

- 1 Get the site's rules before anyone goes**
Ask the site security authority for the regulations that apply, including any restrictions on personal phones, cameras, storage in vehicles inside the perimeter and movement between areas.
- 2 Brief each person before they arrive**
Cover the rules for that site and the devices they may carry, and record the briefing.
- 3 On site**
Identification displayed, own credentials used at every access point, working only in the areas authorised, and working papers kept on the person or secured.
- 4 Photographs**
Agree in advance what may be photographed. Anything captured by accident outside that scope is reported and deleted.
- 5 Before leaving**
An end of day check that nothing has been left behind, on site or in a vehicle.

Where a site needs escorted access or security clearance for your staff, arrange it with the site before the work starts. Guide 3 explains screening and clearance.

END OF LIFE

Destruction, return and loss

Destroying material

The MOD conditions require OFFICIAL and OFFICIAL-SENSITIVE material to be destroyed "in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces". A cross-cut shredder in the office meets that for paper. Where a disposal company is used, keep its certificate of destruction. Devices and removable media are covered in Guide 5.

Returning material at the end of a contract

Customer material is returned when the contract ends, or destroyed where the customer directs. Record which was done and when, and keep to the retention period the customer states. Drawings and reports left in project files after a job has closed are easily overlooked.

When something is lost

For MOD work, the conditions say the supplier "shall immediately report any loss or otherwise compromise" of defence related classified material. Report it to the customer and to the Defence Industry WARP (Warning, Advice and Reporting Point). For central government work, follow the route in your contract's security schedule, which will normally be the contract manager.

Report first and investigate afterwards. A loss reported quickly gives the customer time to act, and shows that the organisation's reporting works.

EVIDENCE

What this area should produce

A customer's security team, or an assessor, will want to see that the arrangements exist and that people follow them.

Record	What it shows
A list of storage locations for each holding	Where material is kept and who can reach it
Keyholder and combination records	That access to storage is controlled and reviewed
Site regulations and briefing records	That staff knew the rules before they arrived on a site
End of day check records	That site discipline happens in practice
Destruction certificates and return records	What happened to material when it was no longer needed

Where this area meets the others

Physical security depends on the people who hold the keys, which is personnel security, and much of the material it protects now sits on devices, which is information and cyber security. A locked cabinet protects the paper in it and nothing else.

HOW THE MARK LOOKS AT THIS AREA

Under the Westmark Defence Supplier Mark, physical arrangements are examined where they protect controlled material, at your own premises and on government sites. The assessment does not include a general security survey of your buildings.

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.