

PROTECTING GOVERNMENT INFORMATION · GUIDE 3 OF 6

Personnel security

Screening people before they are given access to government material, and looking after that access for as long as they hold it and after they leave.

WHERE THE REQUIREMENTS COME FROM

Who may have access, and on what basis

Every other area of security relies on the people inside it. Personnel security decides who is given access to government material, and keeps that decision under review for as long as they hold it.

Source	What it asks for
Baseline Personnel Security Standard Version 7.0, June 2024	Pre-employment checks for everyone who works for government, contractors included. It is the baseline for access to OFFICIAL material, including OFFICIAL-SENSITIVE.
Central government contracts Security schedule	The screening the buyer requires for staff working on the contract, set out in the schedule and recorded in your Security Management Plan.
MOD contracts Contractual Security Conditions, Annex B to Industry Security Notice 2026/04	Access confined to people with a need to know who "have been made aware of the requirement to protect the material". Basic recruitment checks in line with the Baseline Personnel Security Standard.
Official Secrets Act 1989 and National Security Act 2023	The MOD conditions draw a UK supplier's attention to both Acts, and staff with access should be told they apply.
National security vetting United Kingdom Security Vetting	Counter Terrorist Check and above, only where the contract or a site requires it. It needs a sponsor and cannot be applied for by an individual or company alone.

The Official Secrets Act 1989 applies to government contractors as well as Crown servants, and its offences cover people who have been contractors as well as those who still are. The duty stays with a person after they leave your organisation.

BEFORE ACCESS

Screening and clearance

The Baseline Personnel Security Standard

The standard sets four checks: identity, right to work in the UK, employment history and criminal record, which covers unspent convictions. Employment history covers at least the three years before the check. The criminal record check is a basic disclosure, which shows unspent convictions only.

- **It is a recruitment check.** The standard says plainly that it "is not a national security vetting (NSV) clearance". Nobody should describe a baseline check as being cleared.
- **It does not expire.** A completed check does not need repeating unless something changes, such as a break in employment of more than twelve months or a declared change in circumstances.
- **It can be outsourced.** The standard allows an employer to use a screening provider for part or all of the process. The employer still decides who is given access.
- **It comes before access.** Complete the checks before anyone sees government material, and record the date and outcome for each person.

National security vetting

Some contracts and some MOD establishments need staff to hold a clearance. The customer or the site will say which level. Before anyone is sent, check that their clearance is at the level required and in date. Where a person does not hold the clearance a site needs, the site security authority may agree an escort arrangement. Agree it in writing with the site before the visit, and never assume one will be available.

Proportionate for a small business

A small firm can run the four checks itself using the Baseline Personnel Security Standard guidance and a basic disclosure application, and keep the results on one sheet per person. The test is that the checks happened before access and that the record shows it.

BRIEFING

Making people aware of what is expected

The MOD conditions only allow access to people who "have been made aware of the requirement to protect the material". A briefing, given before access and recorded, is how a supplier shows that has happened.

What a good briefing covers

- What OFFICIAL-SENSITIVE means, and how to recognise material that carries the marking
- The customer's own conditions for the contract, including anything unusual in the Security Aspects Letter
- Storage, clear desk and home working rules, from Guide 2
- Which devices and services may hold the information, from Guide 5
- How to report a loss or an approach, and the promise that a report made in good faith will not be punished, even for a mistake of their own
- For site work, the rules of the particular establishment

The statutory notice

Staff with access should be told that the Official Secrets Act 1989 and the National Security Act 2023 apply to information connected with the contract. Keep a signed record that each person received the notice. Where the contract or Security Aspects Letter gives a declaration in a particular form, use that form.

Keeping it current

Brief again when a new contract brings different conditions, or when someone moves onto government work from other duties. Written in plain language and kept short, a briefing is far more likely to be followed.

WHILE PEOPLE HOLD ACCESS

Aftercare, reporting and insider risk

A check is a picture of a person on one day. Circumstances change, and the Baseline Personnel Security Standard notes that although a check cannot be withdrawn, the risks that arise afterwards still need to be managed.

Changes in circumstances

Ask people with access to tell you about changes that could bear on it, such as serious financial difficulty or an approach from someone taking an unusual interest in their work. Give them a confidential route to do so, and record how each report was handled. For anyone holding a clearance, the vetting authority will have its own reporting requirements, which apply as well.

A reporting culture

People report what they believe will be dealt with fairly. State clearly that there is no penalty for reporting in good faith, including someone's own mistake, and treat a report that turns out to be nothing as a report working properly. An unreported approach or near miss is a gap that no screening check can close.

Insider risk

The National Protective Security Authority publishes guidance on insider risk. The practical points for a supplier are to give each person access only to what their work needs, and to act early and fairly when behaviour or access patterns change.

LEAVERS, MOVERS AND SUBCONTRACTORS

When people leave, move on or come from elsewhere

Leavers and movers

- 1 Remove access on the day**
Accounts and building passes are removed on the day the person stops working on government material.
- 2 Recover what they hold**
Devices, tokens, keys and any paper are returned and checked against the records. Change combinations they knew, as Guide 2 describes.
- 3 Remind them of continuing duties**
A short written reminder that the Official Secrets Act and the National Security Act continue to apply after they leave, signed where possible.
- 4 Record it**
Keep the completed leaver checklist with the person's screening record.

Subcontractor staff

Anyone working on the contract through a subcontractor needs the same screening, clearance where required, briefing and statutory notice as your own staff. Confirm the position for each named person. A general assurance that "all our staff are checked" does not tell you who is on your job.

Agency and temporary staff are covered by the Baseline Personnel Security Standard in the same way as permanent employees. If they will see government material, they need the checks first.

EVIDENCE

What this area should produce

Record	What it shows
A screening record for each person with access	That the four checks were completed, and when
Clearance records with expiry dates	That clearance was current when each person was given access
Signed briefing and statutory notice records	That people were made aware before access
Written escort arrangements	That sites agreed access for people without clearance
Change of circumstances and reporting logs	That aftercare and reporting happen in practice
Leaver checklists	That access was removed and equipment recovered

Where this area meets the others

A screened person with an unmanaged laptop, or a vetted engineer who leaves papers in a car, shows why personnel security cannot stand on its own. It sets who may be trusted with access, and the other three areas decide what that access looks like in practice.

HOW THE MARK LOOKS AT THIS AREA

Under the Westmark Defence Supplier Mark, personnel security is checked person by person across a sample of engagements, including subcontractor staff. Giving someone access without the screening that access requires is one of the conditions that 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.