HM Government

Maintaining Security Clearances

A guide for staff and contractors

National Security vetting provides a valuable snap shot of an individual at the time the checks are completed, and organisations also need to maintain ongoing confidence in vetted staff and contractors. Vetted individuals, line managers, and security controllers/managers will have an important role to play in this.

This guide is to inform you of your responsibilities after you have been vetted. It should be read in conjunction will local policies and security briefings.

Why have you been vetted?

You have been vetted because your role requires you to have access to sensitive information or assets or places you in a position of trust. You should have been briefed by your security unit and/or line manager on the security concerns and mitigations in place specific to your role.

Your vetting information provided by your organisation will have details of how long your clearance is valid and other relevant guidance. It is important that you keep these details safe as you may be asked for them at various points. In order to maintain your clearance **you should**:

- ✓ Understand and adhere to local security arrangements.
- ✓ Comply with requests to review your clearance, completing required documentation in a timely manner and fully co-operating with the review process. If you hold a DV (SC in specific instances and as determined by your department) you must complete an Annual Security Appraisal Form.
- ✓ Report any changes in circumstances to your line manager, personnel security team or Security Controller/Manager. A change in circumstance may include living with someone new, a divorce, your financial situation, or conflict of interests (e.g. loyalties or personal relationships potentially at odds with your project/work). Any information you believe could potentially affect your security clearance should be reported. You may be required to complete a Change of Personal Circumstances form
- ✓ Create and contribute to a positive environment in which security is given appropriate priority.
- ✓ Raise any concerns about individual or organisational practices that are in breach of security procedures in the most appropriate way.

You should not:

- ❖ Act in a way that breaches the Civil Service Code or your company's own codes of behaviour.
- ❖ Seek to conceal mistakes, security incidents or breaches. Not reporting an incident will always be dealt with more strongly than taking responsibility.
- ❖ Disclose your level of security clearance online or on social media profiles.
- ❖ Leak information intentionally or unintentionally through failing to protect data and assets entrusted to you. If you have concerns about an activity or individual, speak to your local security team, Security Controller, Line Manager or HR as appropriate.
- ❖ Be negligent of security considerations when working at home, offsite or remotely.

Individuals who handle classified information owned by international partners (e.g. NATO, EU, foreign Governments) are subject to specific arrangements and controls. If this applies to you, please consult your security official for appropriate guidance. Further information is available on https://www.gov.uk/government/publications/international-classified-information-security-clearance

A full summary of vetting policy and processes is available at https://www.gov.uk/government/publications/hmg-personnel-security-controls

Any enquiries regarding this publication should be sent to GSSmailbox@cabinet-office.x.gsi.gov.uk