#Ongoing Personnel Security

Security clearance is a snap-shot of an individual at the time they make their application. Therefore, it is essential that employees are proactively managed using effective ongoing personnel management processes.

When staff are inducted, they are advised of their security responsibilities. Line managers also have a key role in ensuring the security of the department, including personnel security of the people they manage. This is best achieved by following the guidance in this document.

**Parent topic:** [Personnel security clearances](personnel-security-clearances.md)

##Line Manager Responsibilities

* Brief your staff, including contractors, on local and departmental security arrangements and policies as part of their induction.
* Get to know your staff, including contractors who might only be employed for a temporary basis. This is so you can recognise any changes in their behaviour which might impact on the security of the organisation.
* Do not ignore any concerns you have for fear of not knowing what to do. See elsewhere in this guidance for further details.
* Where appropriate, deal with any concerns by talking to the individual, your manager, or HR.
* Create a positive climate in which security is given priority, and individuals are encouraged to discuss any concerns before they become security problems.
* Be a good role model for all your staff, and display good security behaviours.
* Remind all staff with security clearance (CTC, SC, or DV), that they **SHALL** [report changes in personal circumstances](reporting-personal-circumstance-changes.md).
* Remind all staff that they **SHALL** notify the [security team](#contact-details) if they are travelling to certain countries referred to in the [Accessing MoJ IT systems overseas](accessing-moj-it-systems-from-overseas.md) guidance.
* Ensure you are aware of any relevant caveats, or aftercare measures, for staff with security clearance (CTC, SC, or DV), or other security guidance relating to your staff or contractors. Where relevant, make sure your successor is made aware of these requirements if or when you leave your post.

While holders of NSV clearance **SHALL** be aware of their responsibilities, as a manager you **SHOULD** be aware of these points:

* Holders of CTC, SC, and DV are expected to maintain the highest levels of personal integrity, honesty and discretion. They **SHOULD NOT** place themselves in positions where they could be open to compromise, pressure, or improper influence.
* Notwithstanding any set duration, security clearances **CAN** be reviewed at any point if there is a relevant change of circumstances, or new issues come to light.
* Holders **SHOULD** be aware of when their clearance expires, and apply to renew in time.
* Holders **SHOULD** adhere to Ministry of Justice (MoJ) [on-line social media policy](protecting-social-media-accounts.md). Holders **SHOULD NOT** publish their security clearance on-line, including on social networking sites.

##Dealing with concerns

During your time as a line manager, you might notice unusual behaviours in some of your staff; they might behave out of character. It could be that someone else reports their unusual behaviour to you. It is your responsibility to engage with that individual promptly, and address any concerns that you have, or that are brought to your attention. Addressing areas of concern early on can prevent potentially damaging behaviour.

When speaking to an individual, remember:

* Your role as a line manager encompasses security, which means there is a duty of care not just to the individual but also the wider team.
* Vetted individuals **SHOULD** be encouraged to approach their line manager to discuss issues of concern. Early discussions allow appropriate action to be taken, and for support to be provided where appropriate.
* Dips in performance or changes in attitude might be an indication that staff have a wider problem or concern. Do not make assumptions, but do think about mitigations and support to prevent potential security implications.
* Do not put off talking to an individual for fear of not knowing what to do or say.
* Unusual behaviour might be nothing to do with security issues, but might be for several reasons. Listen to the person, and, if possible, offer your support. It might be appropriate to refer them to a [support group available within](/guidance/hr/support-and-wellbeing/employee-assistance-programme/) the MoJ.

For more information, see the MoJ [Support and wellbeing](/guidance/hr/support-and-wellbeing/) resources.

Managing security clearances requires active conversations between managers and individuals throughout the year, and prompt reporting of any issues of concern: [Reporting personal circumstance changes](reporting-personal-circumstance-changes.md). Whilst there are formal renewal periods, clearances may be reviewed, suspended, or withdrawn at any time.

##Managing contractors or consultants

As with any staff, managers are responsible for ensuring that the appointment of contractors or consultants meets MoJ security requirements, and that ongoing personnel security is maintained throughout their stay in the MoJ.

Managing a contractor or consultant is normally similar to managing a permanent member of staff. However, given the sometimes transient and flexible nature of a contractor or consultant’s work pattern, managers **SHALL** pay more attention to them in terms of recruiting and security responsibilities.

There is a good chance that a contractor is not familiar with the MoJ’s security procedures and practices, or even the MoJ’s [Intranet site](/). They might not be aware of the threats faced by HMG, or the specific governmental department for which they work. Advise them that Government work **SHALL NOT** normally be carried out on [personal IT devices](personal-devices.md).

##Summary

* Prior to their appointment, contractors or consultants **SHALL** be security cleared to the appropriate level for their specific role.
* Only a permanent employee (civil servant) can sponsor a security clearance.
* Only a permanent employee (civil servant) can act as a sponsor for the issuing of a building pass. Appropriate security clearance **SHALL** be obtained before sponsoring an application for a building pass.
* “Escorted” visitor passes are exclusively for the use of visitors. Contractors or consultants paid by the MoJ are not visitors, and **SHALL NOT** be issued with a visitor pass. They **SHALL** be cleared in advance of them starting work, and issued with the correct pass.
* When transferring security clearance from another Government department, [Cluster 2 Security Unit](mailto:contactus@cluster2security.gov.uk) **SHALL** confirm if the security clearance is valid and current. If not, a new security clearance application **SHALL** be started.
* Holders of CTC, SC, or DV **SHALL** [report changes in personal circumstances](reporting-personal-circumstance-changes.md).
* Remind all staff that they **SHALL** [refer to the travel abroad guidance](accessing-moj-it-systems-from-overseas.md).
* Ensure contractors, like all staff, are aware of [MoJ security policies](https://ministryofjustice.github.io/security-guidance/), and check their understanding. Make sure they are briefed on good security behaviours, and act as a role model.
* Ensure they are aware of the MoJ [on-line social media](protecting-social-media-accounts.md) guidance and understand the need to avoid publishing their security clearance on social media.
* Create a positive environment in which security is given priority, and individuals are encouraged to discuss concerns before they become serious problems.
* As part of your role, you **SHOULD** seek to get to know your contractor or consultant, and discuss any behavioural changes.
* Although contractors often have a short contract, that might or might not be renewed, they are still given security clearance for a number of years: 5 years for CTC, and 7 years for SC and DV. If their contract period is less than the renewal cycle, then you **SHALL** notify [your local National Security Vetting Contact (NSVC)](/guidance/hr/recruitment/security-vetting/vetting-contact-point-vcp/) when the contractor leaves, so that their security clearance can be terminated.

##Contacts

For any further questions relating to security, contact: [security@justice.gov.uk](mailto:security@justice.gov.uk), or for security advice, contact the [Cyber Assistance Team](mailto:CyberConsultancy@digital.justice.gov.uk).

##Feedback

If you have any questions or comments about this guidance, such as suggestions for improvements, please contact: [IT policy content](mailto:itpolicycontent@digital.justice.gov.uk).