CPNI
Centre for the Protection of National Infrastructure

PERSONNEL SECURITY AND CONTRACTORS

A GOOD PRACTICE GUIDE FOR EMPLOYERS

July 2014

Disclaimer:

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

© Crown Copyright 2014

Table of contents

Executive summary

Most organisations utilise contractors in one form or another. From an independent specialist working on a particular project, through to the use of a third party company providing a team to fulfil a function, contractors are part of everyday working life.

These contractors typically have the same access to an organisation's assets, including those deemed most sensitive, as directly-employed employees and yet on some occasions in some organisations, contractors are not always required to abide by the same personnel security requirements. While this may be a business-driven decision, potentially this could leave an organisation open to risk.

CPNI recommends that organisations use the same personnel security measures with contractors as they would with their directly employed staff. But, it is recognised that at certain times, business pressures may force organisations to use reduced or alternative measures. On these occasions, it is up to the organisation to make a risk assessment as to why they need to downgrade their personnel security standards and what alternative measures can be used instead.

Regardless of what decision is made, it is the employing organisation which owns and needs to manage effectively the risk of granting the contractor access to its sites and assets, not the contractor organisation or agency. The employing organisation also has a responsibility to ensure good security practices are in place and are followed by all staff.

Where contractors are usually given access to the same organisational assets as employees in similar roles, they can have the same impact if they use their access for unauthorised purposes. Potential challenges can include:

- timescales for recruiting contractors can often be tight. This can result in pressure to overlook some pre-employment screening measures, especially if it is anticipated they will be employed for a short time;
- income from contract work can be irregular, which can be a motive for unauthorised activity for financial gain;
- a contractor's primary loyalty may not necessarily be to the employing organisation and their commitment to security may be diminished;
- a contractor feeling that they are not fully part of the team within which they are working;
- a contractor may work in competitor organisations consecutively or simultaneously;
- contracts can be renewed or extended to the point where a contractor can work in an organisation for many years, often with little or no re-screening;
- a contractor may move between departments with the new department not being aware of security constraints that apply to the contractor;
- a contractor may be poorly supported by the organisation that contracted them, who may not see the same responsibility to provide assistance, welfare support or monitoring to non-permanent staff.

This is not a guide to the secure outsourcing of processing or technologies to third party suppliers. While there are equally applicable security measures, such as ensuring that contracts contain security provisions and that audits should be carried out, guidance relating to outsourcing is covered elsewhere on the CPNI website.

Introduction

The aim of this guidance

This guidance provides information about good practice in the secure use of contractors for any organisation. It provides a useful supplement to existing procedures, and for those who are considering introducing new or enhanced personnel security measures.

In this guidance, a contractor is defined as an individual who is not an employee of the organisation, but who has a direct or indirect contractual relationship to provide services to the end user. A contractor may therefore be an individual worker engaged directly under a contract for services or an individual worker engaged to work through an agency. Additionally in large or complex projects, an organisation may engage a third party company, as opposed to an individual, to complete a project or supply services. This company will supply their own staff and may in turn recruit further levels of subcontractor.

The guidance is not intended to replace an organisation's existing policies, but rather to confirm and supplement them. It has been designed to sit alongside other CPNI personnel security products and is aimed at contract managers, human resources managers, line managers and anyone else who may be responsible for the recruitment or management of contractors.

Why is personnel security important?

Personnel security is a system of policies and procedures which seeks to:

- reduce the risk of recruiting staff who are likely to present a security concern;
- minimise the likelihood of existing employees becoming a security concern;
- reduce the risk of insider activity, protect assets and, where necessary, carry out investigations to resolve suspicions or provide evidence for disciplinary procedures;
- implement security measures in a way that is proportionate to the risk.

Working with government and industry, CPNI has produced extensive guidance on personnel security to help mitigate the threat of an insider in the workplace. An insider is a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes. This can include permanent, temporary or contract workers.

This document should be read in conjunction with other guidance published by CPNI, in particular:

- *Personnel Security Risk Assessment: a guide*
- *Pre-Employment Screening: a good practice guide*
- *Ongoing Personnel Security: a good practice guide*
- *Holistic Management of Employee Risk (HoMER)*

These, and other CPNI personnel security guidance documents, can be downloaded from www.cpni.gov.uk

Contractor case study

When contractors go bad…

Organisation X is in a competitive market place, where its intellectual property is unique and highly valuable. Organisation X requests that contractors are screened to an enhanced standard by their parent company, but national security vetting clearance is not required.

Peter, aged 29 and earning in excess of £100,000 per annum, was employed as a software engineer on contract to Organisation X. Due to the urgent business requirement of hiring someone with Peter's skills, a decision was made to proceed without reassurance that the enhanced screening by the parent company had been carried out.

Immediately upon starting his contract Peter was given privileged access to some of the IT systems and he went on to work for the company, with this access, for three years. At no point was any decision made to go back and audit the pre-employment screening Organisation X normally required of the parent company.

Over the three years, Peter achieved his targets; however, he had a number of conflicts with line managers and colleagues. He was known to be a loner, socially awkward, with outspoken but inconsistent views. He was recognised as challenging to manage because he would directly question decisions, even by the most senior member of Organisation X and often refused to follow company policy and procedure. He would often display behaviours that suggested that he thought himself to be technically superior. After one particularly unpleasant exchange, Peter was given a formal warning by his line manager and forced to make a written apology. Peter did not react well to this and was observed using his social networking sites to blog about his unfair treatment. Soon after, Peter resigned from his parent company and left Organisation X mid-contract.

A few months after his resignation, disparaging stories about Organisation X began appearing in the media and several websites were found to contain data that would give the company's competitors a market advantage.

Following an internal investigation Organisation X traced the source of the leaks to Peter. Further investigation showed that:

- Peter's previously unchecked CV contained a number of inaccuracies and embellishments regarding qualifications and career history;
- Peter was dismissed from a previous employer for misconduct, but this information was not relayed to Organisation X;
- Peter had gained privileged access to a number of IT systems that he did not require for his role. He had used a combination of manipulation and bullying of colleagues to acquire this access and exploited the weaknesses within Organisation X's audit and monitoring procedures to do so without drawing attention to himself;
- line managers in Organisation X had often knowingly turned a blind eye to Peter's counter productive workplace behaviours which endorsed Peter's view that he was in the right. He was not made aware of his unacceptable behaviour until it had reached a very serious level where the punishment had to be escalated to a formal warning.

The recruitment process

Preparation

There may be any number of reasons why an organisation chooses to employ contractors, but there needs to be one clear policy as to how to go about doing so and how the contractors will be then managed once employed. This will ensure that all contractors are employed using common personnel security processes and are properly supported with a view to meeting not only just security responsibilities but other legal requirements, such as health and safety.

Ideally, one department, such as procurement or security, should be accountable for the security arrangements for contractors. A senior member within the relevant department should be identified to lead the process and work with all relevant parts of the organisation and the contractors to ensure compliance.

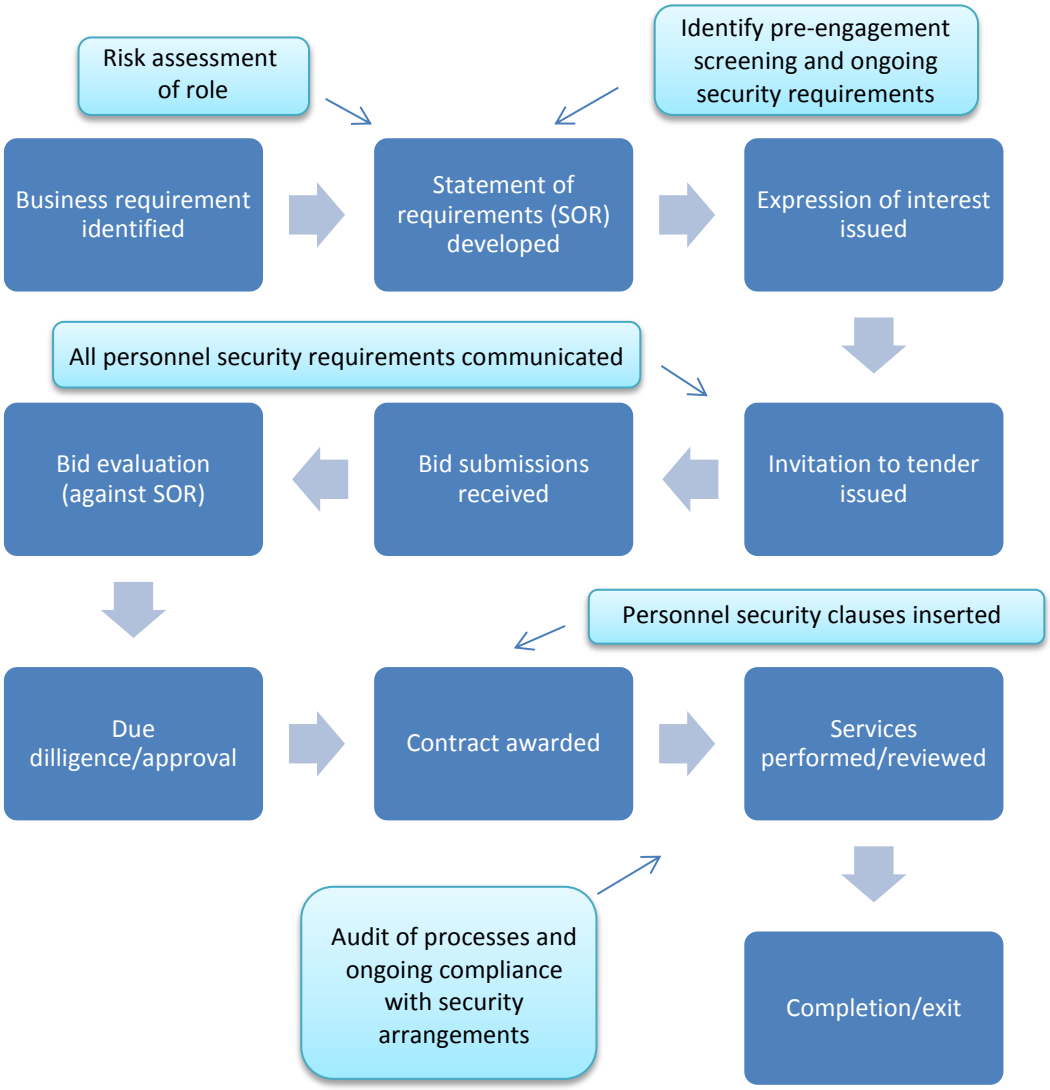
However, for most organisations, a number of different departments will each have a part to play in the contracting process. For example, human resources, procurement, information security, security, legal and the individual business area could all potentially be involved in the recruitment of a contractor.

Whichever way an organisation handles the recruitment process, it is important that there are consistent messages and policies around security. This will help ensure that when the contractor is recruited, they will fully understand all of the necessary requirements of the organisation.

Additionally, regular communication with the contractor throughout this process should help identify any pre-contract issues and then ensure their swift resolution.

The procurement process for the engagement of contractors will differ between organisations, however as a general guide the diagram overleaf illustrates where contracting authorities should be considering personnel security provisions as part of the procurement process for contracting staff.

Personnel security in the contract cycle



Responsibilities

Any agreement for work between the organisation and the contractor should be explicit in what is required from both parties throughout the contract.

Responsibilities for the organisation may include:

- to include the requirements for background checking within the contract;
- to ensure audits are completed/assurance gained;
- for some higher risk roles, a requirement to ensure that background checking forms part of the questions during the tender process;
- to clarify requirement for ongoing/annual personnel security checks/reviews;
- to provide guidance around tolerance roles, such as what will the organisation will and won't accept in terms of an adverse check.

Responsibilities for the contractor may include

- to confirm that the required level of checks have been undertaken;
- to retain records and make available as requested;
- to remove from the contract those individuals whose adverse checks mean that they are not suitable;
- to highlight changes which may make the person no longer suitable – such as a new conviction.

Ideally, if granted access to the same information and location, contractors should be subject to the same pre-employment screening, right to work and ongoing personnel security measures as their permanent counterparts. This may include criminal record checks, financial checks or, where necessary, national security vetting. The nature and the level of the pre-employment screening and vetting standards should be clearly explained in the contract. In the event the contractor's standards differ from those of the organisation, a decision needs to be made about how the shortfall can be addressed.

In some instances, an organisation will require an assurance and evidence from the contractor's parent company that adequate pre-employment screening has taken place. On other occasions, the organisation may choose to carry out its own additional pre-employment screening, regardless of what the contractor may have previously undergone. These issues should all be resolved during the drafting of the agreement between the organisation and the contractor.

A system should also be put in place to confirm that the contractor who arrives to work in the organisation is the same person as the individual/team that has been supplied and 'screened' to work on the contract.

In some cases, a contractor may have to be in post without meeting the organisation's usual standards for security clearance. This may happen where there is an urgent requirement for the contractor to begin work, or where the results of the pre-employment screening are not entirely satisfactory but the need for the contractor's expertise is such that they are employed anyway. In such cases, a risk assessment should be conducted and measures put in place to mitigate that risk.

For more information, read CPNI's Pre-employment Screening Guidance.

A personnel security risk assessment will also inform decisions about ongoing personnel security measures, helping to ensure that they are proportionate to the risk of contractors acting maliciously in post, such as escorted access or restrictions on working hours. It is important that these measures are then implemented.

For more information, read CPNI's Personnel Security Risk Assessment Guidance.

Where relevant, contractor access should be limited physically by zoned/controlled access. Contractors should be issued with a separate, distinguishable pass to permanent staff (such as colour and/or orientation), which should contain a recent photograph of the contractor. Permanent staff should be made aware of any differences between their and contractor passes.

When hired, contractors should have some form of organisational induction. While this may not be to the same level as employees, it would be appropriate to give the contractor the same security reminders and updates. This will help them to understand why security is important, and how they can contribute to the organisation's security culture.

Contracting and the government

Government departments use a similar process to the private sector for hiring contractors. But they should also be conversant with the requirements set out in HMG Baseline Personnel Security Standard, HMG Personnel Security Controls and the Security Policy Framework documents. Government departments and agencies may also wish to refer to the Crown Commercial Service model contract requirements.

It is the responsibility of a contractor who has previously received national security vetting to ensure that they provide information to the vetting authority about any change of circumstance that might prompt a review of their vetting status, including marriage, civil partnership or divorce.

The contractor should also be aware that the organisation that employs them should ensure that their vetting status is verified with the relevant vetting authority. This applies not only to contractors working for the government but also for those organisations which are sub-contracting on large projects that require national security vetting.

Ongoing security management of contractors

Management

Local managers from the organisation's permanent staff should be responsible for contract workers. This may be one-to-one line management or, in larger projects or organisations, a line manager may oversee groups of contractors. The level and nature of ongoing security management should be clearly defined and agreed before the contract is agreed.

Where contractors have access to government assets, the local manager will be responsible for completing Annual Security Appraisal Forms (ASAF) as required by the Security Policy Framework and ensuring the individual is aware of relevant security processes, updates and changes to security practices and is involved in the wider security culture of the organisation. This is important as individuals' circumstances may change post-vetting and it is the contractor's responsibility to notify the vetting provider of any changes to personal circumstances. Managers must also ensure that they effectively manage any caveats associated with vetting clearances.

The contract between the organisation and the contractor should set out standards of behaviour which the contractor is expected to observe, as well as monitoring requirements such as, in the government's case, ASAFs. Contractors should be expected to commit to policies governing acceptable use of email and the internet, obligations toward data protection, security policies, and the organisation's gifts or hospitality policies.

Contractors should also, wherever relevant, be required to undertake the same mandatory training as employees in the organisation, such as security policy refresher e-learning. This is the same principle as undertaking site or system specific Health and Safety or Business Continuity training and should be recognised as such.

Some contractors do not work on the organisation's premises but at home or at third party sites. They may, as a result, be subject to lower levels of supervision, and feel less involved with the organisation and their colleagues. Face-to-face meetings between contractors and their line manager should be held as often as is practical. As flexible and remote working practices increase, both the organisation and the contractor need to ensure they maintain positive and regular engagement that includes messaging on security responsibility and awareness.

For more information, read CPNI's Ongoing Personnel Security and Personnel Security in Remote Working guidance.

Contingency measures

The organisation and contracting company/agency (or the contractor, if no agency is involved), should agree a procedure for providing temporary replacements when the contractor is unavailable. These arrangements should be included in the contractual agreement. The organisation should decide what additional personnel security measures are required when the replacement contractor visits the premises or has access to other assets.

Audit

Organisations should specify the right to audit pre-employment screening and ongoing security requirements with all companies/agencies in the contracting chain. This needs to be agreed upon before the contract is signed and include agreements for what will occur should standards not be met. The audit process should be as transparent and independent as possible.

Exit process

Contractors should be subject to the same procedures as the organisation's directly-employed staff when they finish their contract. This must include provisions for revoking physical access to premises, the return and deactivation of all passes, keys and IT tokens, and the return of any company equipment and documents (physical and electronic) before the individual contractor ceases work with the organisation.

In some cases, the organisation and the contractor may have agreed some form of non-disclosure agreement at the beginning of the contract. This will determine what the contractor can say about the work they completed for the organisation in the future. Any such agreement should be enforceable and clearly understood by all parties involved. In the case of government contractors, this will be the Official Secrets Act.

Reappointment

When a contractor is appointed or reappointed on more than one occasion in the same organisation, it is important not to assume that their circumstances have remained unchanged. This is also true for former employees who are hired as contractors.

To this end, where a contractor has previously been vetted it may be appropriate to consider a review or renewal of an existing clearance, but only where all parties are satisfied that any risks have been considered.

Subcontractors

There will be occasions when the contractor may be required to subcontract aspects of their work to another person or organisation. When this happens, the contracting authority and the first contracted company need to draw up explicit agreements about personnel security arrangements, including a decision about the ownership of any risk associated with the subcontractor.

Conclusion

While there are differences in the employment status of contractors, they should, wherever possible, be subject to the same personnel security measures as regular employees within an organisation. Any deviation from the standard processes should only be taken after an appropriate risk assessment and implementation of mitigation measures.

For more information on personnel security, see www.cpni.gov.uk

Contracting checklist

Risk assessment

- A risk assessment has been conducted to determine the level of insider risk posed to the organisation due to the access to information/assets the contractor(s) role will afford.

Pre-employment screening

- Proportionate pre-engagement screening levels(s) have been agreed that are commensurate to the risk.

Communications

- The level and standard of screening has been formally communicated to the contractor, agency or contracting company (including a mechanism to deal with any adverse information uncovered during recruitment).

Access control

- Agreed access arrangements have been put in place.

Confirming identity

- A system has been put in place to confirm that the contractor who arrives to work is the same person as the individual who has been supplied and 'screened' to work on the contract.

Ongoing personnel security

- Appropriate ongoing security arrangements and policies have been drafted into the contract with clear lines of communication and defined responsibilities outlined (personnel, IT, information and physical).

Susbstitute staff

- A process has been put in place with the contractor, agency or contracting company to manage the substitution of a temporary member of staff when the usual contract staff member is absent.

Auditing

- An appropriate audit mechanism has been put in place to monitor compliance with the required security arrangements of the contract (including pre-engagement screening).

Exit procedures

- An effective off-boarding process has been put in place to ensure that the contractor's access to assets and information has been revoked when it is not longer necessary.

Subcontracting

- The security controls (both pre-engagement and ongoing) demanded by the organisation have been cascaded throughout the entire (sub)contracting chain.

For more information on personnel security, see

www.cpni.gov.uk

Contractor do's and don'ts

To ensure personnel security is appropriately considered by managers, organisations may wish to provide an advisory of do's and don'ts as a reminder of the requirements for the correct way of handling the personnel security of contractors.

DO

Day 1 of contract

- A contractor should have a nominated supervisor/manager. A contractor should not be allowed to roam unescorted prior to them obtaining a building pass.
- The same risk based methodology must be applied to contractors as for employees.
- Contractors should either attend a security briefing/awareness session or a basic security awareness session should be conducted with the contractor (dependent on the organisation's requirements).

During the contract

- The contractor must have access to the organisation's guidelines regarding what will/will not be supported or tolerated by the company and/or knows where to obtain this information.
- The contractor should wear their pass card/ID clearly at all times (where appropriate).
- The manager role is vital in identifying behavioural/performance concerns – therefore contract/project managers should ensure they are aware of how to identify such concerns, and how to report these as appropriate within the organisation.
- Contract personnel must attend relevant on-going security briefings and/or be made aware of updates to policies/procedures that affect them. It should not be assumed that a temporary worker is aware of security/behavioural considerations. The relevant department can advise on whether the briefing/information is relevant to contactors.
- Any penalty clauses that are applied to employees for breaches of policy should be equally applied to contractors.
- Treat the contractor as a valued employee. This is likely to go a long way to enhance their commitment to the company and reduce the likelihood of any unauthorised activity.

On completion of the assignment

- The length of the worker's assignment should be monitored and procedures implemented for terminating IT and buildings access so that the individual cannot gain access to the company's sites or assets on termination of the contract.
- Any documents and items issued to the worker must be recovered in accordance with the company's policy.
- Ensure that personal laptops/smartphones/other devices are erased of all company software, applications and files.
- Contract personnel should be reminded of any non-disclosure or confidentiality agreement that they have previously signed.

DO NOT

Day 1 of contract

- Accept an individual who isn't expected or who has not had the appropriate pre-employment/right to work checks.
- Allow the contractor to use any equipment that they should not have access to, nor have been trained to use.

During the contract

- The contractor must not be given access to any sensitive areas, information or systems without following the correct procedures.
- Sensitive information that he/she does not need to know must not be discussed with the individual.
- Temporary workers should not be moved around or promoted internally without ensuring relevant procedures have been followed; a risk assessment has been conducted; and the contractor has the appropriate level of security clearance. Previous access to IT systems or sites may need to be removed.
- Unless otherwise agreed, contractors should not be given equal status to full time employees when it comes to managing functions that have security implications.
- Any behavioural concerns or breaches of security must not be disregarded. These should be reported to [*insert relevant contact*]

On completion of the contact

- The contractor must not leave the premises with their site pass or any company equipment that should not be retained by them.
- The contractor must not be allowed to leave the premises with the ability to remotely access the company's information.
- Where appropriate, debrief the contractor and use this opportunity to muster all company equipment.