Exit procedures guidance

CPNI
Centre for the Protection of National Infrastructure

CPNI

Centre for the Protection of National Infrastructure

This guidance aims to support security managers, human resources advisers, and others responsible for exit procedures in your organisation, with implementing an effective exit process which helps to minimise the risks posed by employees leaving an organisation.

It is based on expert knowledge, as well as CPNI research, on exit processes within UK Critical National Infrastructure (CNI) organisations and gives an example of an exit procedure process which you can tailor towards your organisation and the particular risks you face.

Introduction

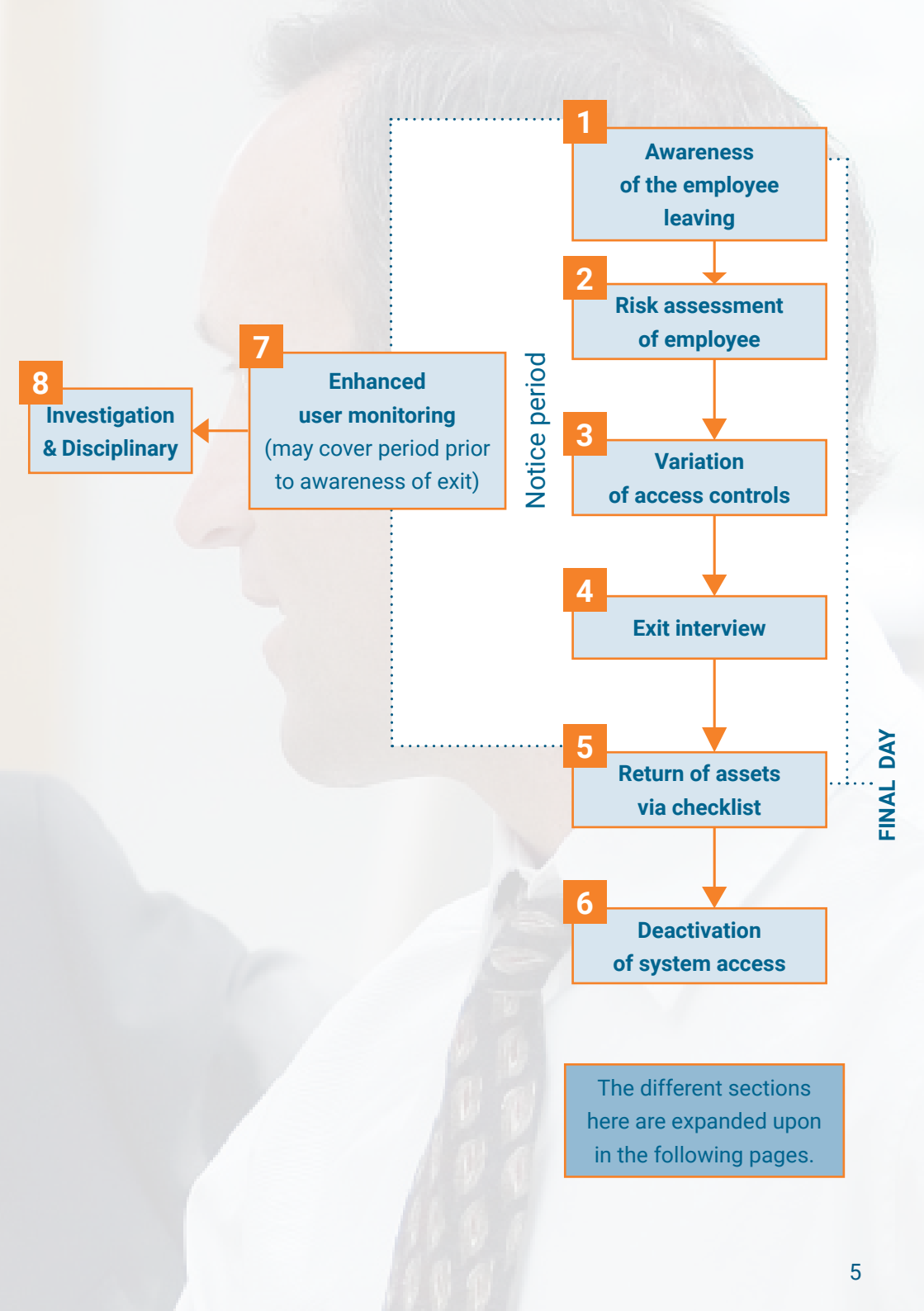
Employees leaving your organisation have knowledge about your operations, assets and security vulnerabilities. Sadly, the circumstances surrounding a departure may not always be amicable between you and your employee. There is a risk that the confidentiality, integrity and availability of critical assets could be compromised if no effective exit and legacy controls are in place, resulting in financial, legal and operational impacts for your organisation.

A formal and thorough procedure for all staff and contractor departures will ensure appropriate actions are taken to protect the organisation without unduly disrupting the employer-employee relationship.

This guidance contains an example of a leaver process which organisations may wish to follow. This process should take place over length of the employee's notice period and includes a post-exit stage of access deactivation.

Contents

Here is an example of a leaver process which organisations may wish to use and tailor to their own business. This process should take place over the length of the employee's notice period and include a post-exit stage of access deactivation.


1
Awareness of the employee leaving
2
Risk assessment of employee
3
Variation of access controls
4
Exit interview
5
Return of assets via checklist
6
Deactivation of system access
7
Enhanced user monitoring (may cover period prior to awareness of exit)
8
Investigation & Disciplinary
Notice period
FINAL DAY
The different sections here are expanded upon in the following pages.

1

Awareness of the employee leaving

There are many reasons why an employee might be leaving an organisation, such as finding new employment, redundancy, change of career and, of course, dismissal . Regardless of how amicable an exit may seem, once a line manager or the human resources (HR) team is made aware of the impending exit, it is important that a process is followed to ensure the organisation is protected and the risk to the assets are minimised.

2

Risk assessment

As soon as a line manager becomes aware that their employee is leaving the organisation, they should assess and manage any risk that the employee may then pose. If necessary, they may wish to consult with security and HR to accurately assess the risk and decide what measures could be put in place. Any measures taken will be influenced by a number of factors, including:

- whether the employee is leaving voluntarily, or as the result of a disciplinary process or redundancy
- if they are not leaving voluntarily, the reason for their dismissal
- whom they are going to work for (e.g. a competitor)
- if they are going to work for a competitor, is this a result of dissatisfaction with the organisation
- their current role and the sensitivity of the organisation's assets which they have access to

3

Variation of access controls

Having assessed the risk for a particular individual, the organisation should determine the best course of action. Broadly, and depending on the employee's contract, these options are likely to include:

- allowing the employee to continue working during their contractual notice period, retaining all their usual access to the organisation's assets
- allowing the employee to work their contractual notice period, but with reduced access to assets and IT
- asking the employee to leave immediately, possibly under supervision, to prevent any unauthorised act while still on the premises. In this situation, the employee should not return for the duration of their notice period
- if appropriate, removing their access to commercially valuable information if they are leaving to work for a competitor

However, it is necessary that any action taken in this regard is proportionate to the risk faced. Unnecessary restrictions during a notice period may cause or enhance any ill-feeling and disgruntlement amongst leaving staff.

4

Exit interview

Exit interviews are a very important aspect of the staff leaving process. Often the employee's line manager and a representative from HR would arrange the exit interview. However, depending on the circumstances, the meeting may be more open and informative if the line manager is not present as employees may be more willing to speak frankly about experience working within their team. It is also important to ensure employees are aware that their honest feedback will not result in any future retributions, such as negative references.

Interviews should be conducted with care and confidentiality. It is therefore good practice for all exit interviews to have a defined structure or format so that they are not reliant upon the skills and experience of the interviewer. Furthermore, a set template would assist in consistently collecting relevant information to help HR identify any trends. Where an employee is leaving as a result of a disciplinary outcome, the final disciplinary session and exit interview are likely to be merged into one meeting.

The exit interview is an opportunity to:

- ask and listen to the employee's reasons for leaving, particularly to any comment on how the organisation may have been responsible for their decision
- ask the employee if they have any comments or observations about the strength (or weakness) of the security culture, measures or procedures in place within the organisation
- recover organisational assets, access tools and identifiers, unless alternative arrangements have been agreed with the organisation
- obtain all passwords or encryption keys for files the employee has been working on
- offer guidance on what to put on professional networking sites regarding employment
- remind the employee of their security obligations under organisational codes of conduct concerning access to assets and intellectual property or (where appropriate) the Official Secrets Act 1989

- to reinforce this, some organisations ask the employee to read and sign a form summarising these points

The timing of the exit interview should be driven by the personnel security concerns. Normally, they are conducted in the employee's final week. However, where the risk is assessed to be high, the interview should be arranged promptly to ensure the employee is aware of their security responsibilities at the start of the notice period.

5

Return of assets via a checklist

It is good practice for organisations to create a checklist documenting what items are required to be returned and any final actions. The checklist should only be signed off once all actions are completed and all assets returned. It is important to also check with previous departments within the organisation where the employee may have worked to see whether they received all assigned equipment back.

Assets to be returned may include:

- security passes and/or identification cards
- company mobile phones
- company laptop and other IT equipment
- company credit cards
- tokens for access to electronic systems
- any books, papers or commercially sensitive documentation
- keys to secure storage areas

If the employee is leaving immediately, they should return all company property within the tightest possible timescales. For items unable to be recovered straight away, a date and method of their return (such as in person or by recorded post) should be agreed with the employee.

6

Deactivation of accesses

Similar to return of assets, a checklist should be used to remove any access a previous employee once had. For this process, it would be useful for there to be a centralised system which can capture individual building and access rights. Things to consider are:

- selectively or completely blocking the employee's user IDs to prevent system access
- deactivating email accounts
- changing passwords to common systems
- deactivating the employee's security pass to prevent physical access to all company buildings
- changing door codes to common areas
- changing combinations to storage areas and/or security containers
- cancelling the employee's signature authority, credit card and expense accounts

Again, the above should only be signed off once all the actions are complete.

7

Enhanced user monitoring

Once the risk assessment is completed, it may be decided that due to access to sensitive information and assets or reasons for leaving, those responsible for protective monitoring should be informed. The risk assessment should dictate what activities should be monitored to reflect any risk posed. Unless for investigations, it will normally be disproportionate to continuously monitor all of the leaving employee's activities.

Such activities which may be monitored include: emailing sensitive or large amounts of information to personal email addresses, exfiltration of commercially sensitive data via removable media, theft of intellectual property, unusual amounts of printing, manipulating information in an act of sabotage, file transfer and accessing the network remotely.

There may be a small window of opportunity between identifying potential indicators of malign behaviour and an employee leaving with valuable information. Therefore, organisations must be prepared to take rapid and proactive action in swiftly investigating any such incidents.

Additionally, the risk assessment may deem it necessary to also investigate the user's activities prior to handing in their notice, as employees intending on exfiltrating information may be wary of additional monitoring during the notice period. A period of 30 days prior to awareness of leaving is recommended as this provides a proportionate balance between a review of historical monitoring data and the resourcing required to do this.

8

Investigation & disciplinary

The monitoring in place may identify some behaviours which are indicative of a malicious insider act. If this is the case, the usual CPNI approach to investigation and disciplinary should still apply – that is, to ensure any approach is proportionate, impartial and formally recorded. It may be useful to have interested parties involved at this stage such as HR, the individual's line manager and security.

However, it is important that those involved recognise the importance of acting fast and so it may be necessary to prioritise investigating this incident and interviewing the individual straight away. The result of the investigation may range from no action if no evidence of wrongdoing is found, through to immediate removal of the employee from the organisation, informing the employee's new place of employment and involvement of law enforcement.

Exit procedures for those unable to return to site

It is not always feasible for employees to return to site in order to fully follow a leavers' process. This would include those on long term sick leave, maternity leave, working abroad or on special unpaid leave. In such situations, organisations should attempt to tailor the above process to ensure that these employees are still given the opportunity to have some type of exit interview and that all company assets are returned.

It is best practice to continue to follow a modification of the above process, such as arranging a day where the exit interview and returning of items could be done on the same day. However this may not always be possible. Therefore, alternative arrangements could involve the following:

- completing an exit questionnaire which allows for employees to still air any grievances which they may have or to give recommendations on areas for improvement
- interviews could be conducted using online video communication
- if convenient, an alternative senior individual in another office could be assigned responsibility and a checklist to collect items
- arrangements could be made for the collection of an item being posted back through a recorded service.