CPNI
Centre for the Protection of National Infrastructure

Security Investigations Guidance

PUBLISH DATE: Spring 2022

CLASSIFICATION: Official

Personnel Security

INVESTIGATING EMPLOYEES OF CONCERN

A GOOD PRACTICE GUIDE

Edition 2: Spring 2022

KEY POINTS:

This document provides guidance to employers on the stages and considerations involved in conducting legal, ethical and fair security investigations on employees of concern. In summary, these are:

- Clear staff policies and procedures outlining responsibilities towards security must be communicated to all staff (including contractors) at induction, and repeated regularly throughout their employment. A breach of these policies and procedures will require action to be taken to determine whether an investigation should be launched.
- Where an internal security investigation is required it should be planned and conducted by a trained investigator who will need to consider the parties to be informed about the investigation, both internally and externally.
- An internal UK based security investigation is not a criminal inquiry and therefore the burden of proof will be on the 'balance of probabilities' and not 'beyond reasonable doubt'. Security investigations taking place overseas may be subject to different rules.
- All investigation actions and enquiries must be recorded to show the reasons for them taking place along with their outcomes. All Interviews must be conducted fairly and transparently, with a written statement of the interview being signed by both parties.
- Evidence should be carefully collected and collated. Sources of evidence may be from face-to-face interviews, protective monitoring of organisations IT systems, corporate electronic media and physical searches conducted in accordance with UK legislation.
- A full report should be shared with whoever is considering the findings of the security investigation and they will convene a disciplinary hearing.
- The person under investigation should be called to a disciplinary hearing and may be accompanied by a staff representative/trade union official or a colleague. The decision of the hearing should be given to the employee as soon as possible, preferably, in writing.
- If there is no case to answer, there should be no further action taken against the employee. If the original allegation against the employee is found to be malicious then a further HR investigation may be launched into those who raised the allegation.
- If there is evidence of wrong-doing then the appropriate sanctions against the employee should be agreed. Sanctions can range from an individual being given advice or training, through to dismissal.
- Following the conclusion of a security investigation the organisation should review the investigation to ensure that, where necessary, policies and procedures are tightened, security awareness is raised and gaps in security are plugged. Please refer to the CPNI Insider Risk Mitigation Framework for advice relating to reviewing risk assessments post investigations.

Contents

Introduction

Many organisations will at some point need to carry out an internal security investigation into the actions of a member of staff. When a security related concern is raised about an employee, organisations can be unsure of how to react, particularly if an accusation of wrong-doing is hard to prove.

The primary duty for any investigator is to establish the true facts, and to be impartial, fair and objective whilst gathering evidence and when dealing with those raising concerns and the employee being investigated. Should litigation follow an investigation and dismissal, one of the employment tribunal's functions will be to examine the reasonableness of the investigation, including it's fairness, objectivity and thoroughness.

Organisations should have policies in place outlining how employees are expected to behave in the workplace. These may be included in the terms and conditions of employment for employees, or in the contracts for contractors. Policies should also outline employee responsibilities towards security (personnel, physical and information/ cyber). Where appropriate, these should state that responsibilities are extended outside the organisation i.e. working at home, on the move or working remotely. In some cases, these responsibilities could be continued for a defined period after the end of employment.

Having policies in place will make it easier to investigate and discipline staff if wrong-doing is proven. For example, issuing an Acceptable Use Policy (AUP) for staff on email usage will make it difficult for an employee to argue that they were unaware they should not have been looking at illegal or offensive material.

Employees should be aware of the organisation's disciplinary procedures. These should be in line with guidance set out by the Advisory, Conciliation and Arbitration Service (Acas) Code of Practice on disciplinary and grievance procedures[1].

Written guidance for investigators outlining the purpose of the investigation is important to guide them through the process. If an organisation operates a zero tolerance policy, there is an obligation to investigate concerns no matter how awkward it might be for the organisation. Any response must be proportionate, and the guidance should stipulate what actions are permitted during the investigation such as: IT monitoring, CCTV footage and searches (both physical and bodily searches, and obtaining approval to carry out searches).

Policies and procedures should be reviewed on a regular basis to ensure that they are reasonable, legal and proportionate.

Organisations such as Acas[2] and the Chartered Institute of Personnel and Development (CIPD) offer a range of courses on managing and conducting investigations and interviews[3].

[1] https://www.acas.org.uk/acas-code-of-practice-on-disciplinary-and-grievance-procedures

[2] https://www.acas.org.uk/

[3] http://shop.cipd.co.uk/shop/cipd-training/courses-qualifications/human-resources?p=3

Preparing for the security investigation

Who carries out the security investigation?

Some organisations will have dedicated investigators; others may need to identify someone who investigates on an ad-hoc basis. All security investigators should be provided with the right training to support them in their role. Investigators should not usually work with the employee under investigation. Also, to ensure impartiality, it is important that anyone involved, or suspected of involvement in the action being investigated, is not involved in the investigation. If this is the case, suitable alternatives should be consulted.

Planning the investigation

Planning the investigation should begin with determining why a security investigation is necessary and proportionate. This can take the form of a 'scope and purpose' document, or an 'impact assessment'. This need not be lengthy: it merely needs to establish the need for a security investigation, for example: 'This investigation is based upon a report that employee X downloaded malware on the corporate IT system, causing a shutdown of equipment resulting in the disruption of critical services.'

Any statement should summarise the requirement in neutral terms which do not suggest that anyone has prejudiced the issues. This helps ensure focus and impartiality in the investigation.

At the scoping stage it is important to consider the nature of the security investigation. Questions to be asked are: will it be sufficient for a simple discreet desktop review or enquiry to take place, where the employee under investigation will never be aware of the enquiries? Is significantly more information needed? What will happen with the information once it has been collected.

The investigator should consider the motivations of those making an accusation – do they have a well-founded concern, are they mistaken or are they just being malicious? If malice is proven, the organisation will need to consider whether disciplinary action is required against those making the accusation.

The investigator should also consider whether there is an obviously innocent explanation to a concern or suspicion. For example, if an employee is working outside normal working hours, is working late in a particular section the norm, is the employee catching up on workloads, are they doing business with others in different countries/time zones, or are they conducting non-work related but legitimate activity?

If it is suspected that a criminal act has taken place, the appropriate law enforcement authority should be contacted as early as possible. They will be able to provide appropriate advice on proceeding with an investigation or take over the investigation as required.

Who should be informed about the investigation?

The decision of who to inform about a security investigation should be taken carefully in order to restrict the circle of knowledge, and to reduce the likelihood of an unauthorised disclosure of information. The CPNI Insider Risk Mitigation Framework provides the governance structure to support security investigations within the workforce. There are various individuals, departments or bodies that it may be desirable for the investigator to consult before, during or after the investigation. In some cases, only a

limited number of people outside the investigation team will be informed; other cases may require a wider circle. Who should be consulted will depend on the investigation, but may include the following:

Directly supporting the investigation	HR	Line Manager	Senior Manager	Security Dept
Required to take action	Finance	IT	Legal	Comms
Acting on behalf of staff member	Union	Staff Body		
Outside Bodies	Police	NCA	CPNI	NCSC

- **Supporting the security investigation** – line managers are usually best placed to provide evidence of observable workplace behaviour and context to the investigator. In the case of the senior manager, they can provide support and direction, especially in the event of adverse publicity or litigation arising from the investigation. HR departments can provide supporting background information and will have a role to play if the outcome of the investigation has an impact upon the employment status of the individual. A Security Department may carry out the investigation and can also provide manual searching.
- **Required to take action** – Finance, IT, Legal and Communications teams help the security investigative team by taking specific actions as required. For example, IT assists by providing IT audits and monitoring. Investigators should inform and take advice from the organisation's lawyers or internal legal counsel, to ensure that the investigation is being conducted in a lawful, reasonable and proportionate manner. If there is suspicion of financial wrong-doing, the financial or accounting departments should be informed as soon as possible to undertake financial audits and to freeze or close accounts. An organisation's Communications Team may be required to prepare press lines to counter press interest/exposure.
- **Acting on behalf of staff member** – if the employee is a member of a trade union or has elected employee representation, a decision may be taken to inform them during the investigation. A representative may accompany the employee at interviews or disciplinary hearings.
- **Outside bodies** – in addition to the police, other organisations such as CPNI, NCSC, the National Crime Agency, should be informed if an investigation finds that the employee may be involved in activities relating to terrorism, espionage or serious crime, but there are insufficient grounds to take action. Employers should appreciate that authorities may only be able to provide advice and guidance and not definitive answers, as this could prejudice other investigations carried out by official bodies.

Interviews

Interviewing sources

A key aspect of a security investigation is to interview the source of the original suspicion/accusation (if known). During questioning, it is important to ask the source how they became aware of the information/incident, and if they know of anyone else who might be able to assist with the investigation. The interviewer should establish whether the source has reported the matter elsewhere, and whether they consent to their identity being revealed to the employee under investigation.

Wherever possible, two people should be present at this interview – one to ask questions, and the other to take notes, ensuring that the responses are recorded accurately and that nothing has been missed. The interviewers may propose, with the consent of those being interviewed, to record the interview electronically. The interviewers should explain the process to reassure and build rapport with the interviewee.

Determining confidence in a source can vary depending upon the level of co-operation given during the interview. The interviewer should establish whether the source is providing information that is distorted, embellished or inaccurate. Further interviews with the source or other witnesses may therefore be required. If the source turns out to be biased and the accusation groundless, an interview will help avoid an unnecessary investigation.

Distinguishing facts from opinions and hearsay

Interviewers often must distinguish between fact, opinion and hearsay. Opinions and hearsay evidence may be permissible in an employment tribunal if they are relevant to the issues. If presented, they should be noted as such and not as a fact.

Where relevant, the interviewees should be reminded that their statements can be verified through, for example, CCTV footage or telephone/IT logs, which may corroborate their evidence.

Documenting the interview

The interviewer will prepare a written record of the interview. The interviewer and interviewee should both sign and date each page of the statement to confirm its accuracy. Any amendment to the statement should be agreed and initialled by both parties.

If an interviewee declines to assist an investigation the investigator should consider whether the information is unreliable, or if the interviewee is fearful of reprisals. The interviewer should be aware that the interviewee may have been complicit in the activity under investigation, either as a willing or unwilling participant.

As most organisations do not have the power to prosecute an employee, they do not need to abide by the tenets of the Police and Criminal Evidence Act 1984 (PACE)[4], which sets out how a criminal interview should be conducted. However, it is recommended that legal advice should still be sought before commencing interviews to ensure there is no likely infringement of the Equality Act or Data Protection Act.

Witness and information protection

As well as providing reassurance to the interviewee regarding the process, the witnesses should be advised that they must keep the information they have reported confidential at least until the conclusion of the investigation. They should also be advised of the privacy rights of the employee(s) under investigation. Making the existence of the security investigation or any of its details public may jeopardise the investigation and breaching confidentiality could lead to disciplinary action.

Interviewing those under investigation

It will be essential to interview the subject of the investigation. The employee may have rights of representation according to the employer's procedures.

A framework for the interview should be planned in advance. As the interview progresses, the interviewer should seek clarification on answers provided or new issues that arise. The interviewer should not expect or aim to extract specific reactions from the employee under investigation. If expectations are set in advance, any new information or change in direction may be difficult to handle.

Many of the practices, such as documenting and verifying information, will be the same as those for witnesses. At the start of the interview it is important to outline the purpose of the interview, what facts are known and what information requires clarification.

Investigators should be trained in interviewing skills, including techniques of building rapport, open and closed questioning and body language.

As with a source interview, the employee under investigation should be offered the chance to sign and date each page of the written statement of their interview.

[4] For England and Wales. Also the Police and Criminal Evidence (Northern Ireland) Order 1989 and the Criminal Procedure (Scotland) Act 1995

The security investigation

This is an internal investigation into a potential breach of the employer's policy, not a criminal inquiry. The burden of proof will be the 'balance of probabilities', i.e. that it is more likely than not that the employee has committed the security breach.

If a decision is made to investigate an employee overtly (see below), they should be notified in writing. The letter should state the nature of any allegation/suspicion, whether the employee will be transferred to other duties during the security investigation or suspended (see below), and if suspended, arrangements for contacting or visiting the organisation or colleagues (e.g. for interviews or disciplinary panels) and possible outcomes following the investigation.

Should an employee under a security investigation be suspended?

Suspension is not a disciplinary sanction; it is part of the investigation process. It is usually considered necessary if it is suspected that the employee under investigation may interfere with the processes or witnesses of the security investigation.

Suspension may not always be necessary. The employer may decide to restrict the employee's access to sites, property or evidence in question, or to move them into another role during the investigation.

The organisation's policies should set out the grounds for suspending an employee. If a decision is made to suspend, the employer should remove and de-activate their ID cards/passes, access control, remote IT access and other necessary materials.

Employers must review suspensions regularly to ensure that they remain justified and appropriate. If the suspension continues for too long or in circumstances where it could properly be lifted, it could justify the employee resigning and claiming constructive dismissal.

Should the security investigation be conducted overtly or covertly?

The nature of the incident will determine whether or not the employee under investigation should be notified of the investigation. Factors determining whether the investigation will be conducted covertly may include:

- The nature and severity of the incident or suspicion.
- Whether the incident constitutes a sustained or ongoing unauthorised act that requires monitoring without alerting the perpetrator.
- Whether the investigation relates to a planned or unauthorised act that has yet to occur.
- The level of additional reporting required, for example CCTV footage or monitoring.

Before a decision is made to proceed with a covert investigation, the investigator should consider whether it is proportionate to do so. Does the seriousness of the wrong-doing justify the level of intrusion merited by a covert investigation into the privacy of the employee under investigation? Any decision to proceed with a covert security investigation must be approved by senior management.

Recording the investigation

Throughout the security investigation, the investigators should thoroughly record all interviews, actions and enquiries undertaken, the reasons for doing so, and the results of the actions/enquiries.

The use of photographs, charts, diagrams and other depictions may be appropriate to illustrate or clarify details of the investigation or actions. Documents obtained during the investigation should be copied, and the originals secured and maintained in an original state and made available for future actions or handed over to appropriate authorities for future evidential value.

Evidence

The collection and collation of evidence is crucial to any investigation.

The evidence required (the who/what/when/why and how) will vary depending on the incident or suspicion being investigated but can include:

- Interviewing sources.
- Examination of audit trails such as telephone call logs, emails or IT activity, created by the organisation's protective monitoring processes.
- Reviewing CCTV footage.
- Overt or covert surveillance of parties involved (covert surveillance should only be used in exceptional circumstances).
- Forensic examination of office equipment used by the employee.
- Reviewing the employee's financial transactions.

Legislation covering evidence gathering can be found at Appendix 1. A list of possible technical and non-technical data sources can be found at Appendix 5.

Technical and IT Monitoring

Technical and IT monitoring is when an organisation carries out systematic or occasional checks on some of its employees. It can take a variety of forms, including:

- **Email** – incoming and outgoing mail, including attachments.
- **Internet use** – detection of attempts to access inappropriate websites or use of social media.
- **IT use** – to detect unauthorised downloading to media such as CD ROMs or USB sticks, access to systems or exfiltration of bulk data.
- **Telephone details** – including numbers dialled, the duration of calls, and the recording of conversations.
- **CCTV** to confirm the employee's presence in a particular area or unauthorised activity.
- **Physical access controls** such as swipe cards, PIN codes or intrusion detection systems, to detect attempted access to prohibited areas.

Covert monitoring is justified when an organisation has good reason to suspect a criminal offence or other offence of a similar severity has taken or is taking place.

Legislation/codes of practice covering monitoring can be found at Appendix 1. For example, the Employment Practices Code states that, before commencing monitoring, an organisation should carry out an impact assessment to ascertain whether the benefits from monitoring outweigh the level of intrusion into the privacy of the individual. The code suggests employers should:

- Target monitoring on areas of highest risk.
- Limit monitoring to traffic data rather than the contents of specific communications.
- Undertake spot-checks rather than continuous monitoring.
- Automate monitoring to reduce the extent to which extraneous information is made available to any person other than the parties to a communication.

Investigators should not accept recordings of conversations from employees or other people who may be trying to assist in the investigation as it may be illegal for them to record such conversations. Legal departments should be contacted for advice on handling such recordings.

CPNI's Legal Considerations Employee IT Monitoring looks at the law relating to Employee IT Monitoring in the UK and 11 overseas jurisdictions.

Organisations must ensure all evidence is stored in a way which guarantees its integrity, both for the duration of the investigation and for any time allowed for appeals or legal challenges following the investigation's conclusion.

Searches

A security investigator should be allowed to conduct searches of the organisation's property, locations, offices, vehicles, desks, computers and storage lockers etc. This should be included in the organisation's security policies.

However, a body search of an employee, without their consent, may amount to an assault. Where it is imperative that a search be carried out, the employer should consider the gender of the person being

searched and select an appropriate searcher. Where there is a potential criminal investigation, the police should be called immediately. The investigator should not put themselves or others involved in the search at risk.

The timing of the search and those present should be agreed with the organisation's legal and HR departments. Where possible, every effort should be made not to advertise that a search is being undertaken, and there should be as little disruption to the work environment as possible. Searches should be carried out by someone who is trained in conducting searches, and in a way that will not destroy or compromise evidence. Consideration should be given as to whether the search should be conducted in the presence of the employee under investigation.

Where possible, searches should be conducted in the presence of an independent person (for example, a member of HR). They can observe the search and note anything that is removed, particularly personal items. Consideration should also be given to photographing or videoing the search, which can serve as a record of the search process and may be used for evidential purposes. A complete inventory of items located and removed during the search must be completed and signed by any witnesses to the search.

Security investigations overseas

Investigating and resolving security-related concerns about an individual or incident overseas are key aspects of personnel security. However, in some countries the legislation surrounding investigations is vague and it may be unclear whether a particular activity is permitted. Employers must ensure that any action complies with the law within the country concerned, and take appropriate legal advice. Often the police only need to be informed where it is clear that a criminal offence has been committed or where the matter is sufficiently serious to require their involvement.

In general, data protection legislation in the EU places a duty on employers to ensure that any security measures imposed (in particular, communications intercepts or surveillance) are proportionate to the threat faced. Within the EU, although ongoing employee security measures are generally not restricted by law, not all measures are widely accepted practice.

Many countries do not prohibit the monitoring of telephone calls, email logs or financial transaction data, although some restrict collection to information obtained directly from organisation premises or systems. Some countries prohibit search or seizure by any entity other than the police, and in others these procedures are restricted or regulated.

CPNI's Personnel Security in Offshore Centres looks at personnel security measures in countries which are popular locations for offshoring and outsourcing services from the UK, including security measures during employment, the use of formal investigations, and the legal parameters within each country.

Reviewing the progress of a security investigation

Organisations should carry out periodic reviews as the investigation progresses. This can identify whether further avenues of investigation are warranted, if there is insufficient evidence or indication of wrong-doing to carry on with the investigation, or whether the police should be approached with a view to taking over the investigation. Appendix 2 is a checklist that investigators can use to confirm that appropriate actions have been taken during the investigation.

Legal privilege

The employer should remember that legal privilege attaches to all communications between them and their legal advisers. Communications cannot be disclosed without the permission of the client. The privilege is that of the client and not of the lawyer.

The security investigation report and all non-privileged correspondence and communications obtained during the investigation must be disclosed and be subject to examination by a court. This also applies to notes, photographs and other documents collected or used in an investigation.

Following the security investigation

The report

Once the security investigation has concluded, the investigators should prepare their final report and present it to the individual or panel appointed to consider the findings of the investigation. The report should be as concise as possible, and only present the relevant information and facts obtained during the investigation.

Where possible, the investigators should **not** make formal findings or apportion blame. Their role is to present the facts and to allow those making the decision about the employee under investigation to reach their own conclusion. This will require discipline on the part of the investigators to ensure their findings are not prejudiced in any way.

The report may contain the personal opinions of the original source of the information/allegation, and of those interviewed where relevant to the investigation. Such opinions must be identified as those of the person being interviewed so as not to allow the reader to confuse them as facts.

Disciplinary procedures

Employers should follow their established disciplinary procedures, which should be up-to-date, compliant with the ACAS code, and capable of dealing with cases of suspected insiders.

Dismissal

If the employee has committed a serious offence, or if previous stages of the disciplinary process have been exhausted, a decision may be made to dismiss them. Such a decision must be in accordance with the organisation's disciplinary and dismissal policies. Any decision to dismiss should only be taken by a manager who has the authority to do so. The employee should be informed as soon as possible of the reasons for the dismissal, the date upon which their employment/contract will end, the appropriate period of notice, and their right of appeal.

If the employee is dismissed, full and proper exit procedures should be followed, including the revoking of physical and electronic access to sites and systems, and the retrieval of all organisational property.

Further information on handling disciplinary and dismissal issues can be found in the ACAS Code of Practice on disciplinary and grievance procedures[5].

The employee under investigation may resign before the investigation is completed or actions taken. In this event, the investigation should still be completed to determine whether criminal proceedings should follow, to avoid re-employing the same individual at a later stage, to provide an accurate reference to future employers and, importantly, to learn lessons about organisational failures that may need to be addressed.

[5] https://www.acas.org.uk/acas-code-of-practice-on-disciplinary-and-grievance-procedures

Informing the authorities

During or following a security investigation, an employer may believe it necessary to contact the authorities (such as CPNI, NCSC or the Police) about their employee. It is difficult to determine the exact moment when the employer should do this, as each case will be different. However, if the employer's workforce or the public is at risk of serious crime, not telling the Police may damage the employer's reputation or possibly incur criminal liability. For example, employers have a duty to report certain terrorist activity under section 19 of the Terrorism Act 2000[6]. However, the internal security investigation and disciplinary action should continue to its conclusion even where other bodies are involved.

If the employer informs CPNI, we will pass any information to the relevant investigatory bodies, who will then examine the information. Employers should appreciate that it may take some time for an investigation to result in anything conclusive, and there may well be limits on what CPNI can tell the employer.

Informing regulators

If the organisation is regulated, it may be a requirement to inform the regulator of the situation. If the activities of the employer affect other organisations within that sector, the regulator may consider introducing additional measures to mitigate any threat.

Reviewing the security investigation

As soon as possible following a security investigation, a panel of stakeholders should conduct a review of the investigation to ascertain how it progressed, identify any problems that arose, and determine whether existing policies and procedures are sufficient, or require updating. This process should follow the CPNI Insider Risk Mitigation Framework which recommends the organisation's insider risk stakeholders are made aware of the outcome of the investigation and the Personnel Security Risk Register is reviewed so new mitigations can be put in place. For example:

- Additional security measures may need to be put in place e.g. access control or new IT monitoring/audit procedures. These should be communicated to all staff.
- Additional training may be required to enforce the new measures.
- Security behaviours which are desirable to support the organisations security culture may need to be reviewed and enhanced (along with appropriate training) so that staff feel more confident and are able to challenge suspected wrong-doing in the workplace. Actions could include running CPNI's It's Okay To Say programme.
- If colleagues feel that the employee has been treated unfairly, it is possible that this may result in resentment against the employer. Therefore, the organisation will want to consider how to issue security minded communications to staff post an major event.

[6] www.legislation.gov.uk/ukpga/2000/11/contents

Testing

Testing and rehearsing internal processes for a major security investigation is recommended to ensure that the organisation is not unprepared should the worst happen. Realistic Insider risk scenarios for testing can be gained by referring to the organisation's risk register.

Appendices

Appendix 1 – Legislation

When conducting investigations, employers must bear in mind their legal obligations under the following legislation:

Human Rights Act 1998 (HRA) – www.legislation.gov.uk/ukpga/1998/42/contents

Article 8 of the HRA provides for the right to respect for privacy and family life. Individuals' Article 8 rights also extend to the workplace. The amount and extent of evidence collected should be necessary and proportionate in the context of the type of investigation being carried out and the nature of the incident or suspicion.

Data Protection Act 2018 (DPA) – http://www.legislation.gov.uk/ukpga/2018/12/contents**.**

The DPA regulates the way in which personal data (including that which is collected during an investigation) is collected lawfully and processed, stored and destroyed in a fair and proper way. Information collected for the purposes of an investigation should be held for the duration of the investigation, as well as any time allowed for internal and external appeal processes. Part 3 of the Act concerns monitoring at work. The EU's General Data Protection Regulator (GDPR) requires UK employers to demonstrate compliance by design and that they have obtained consent from the employee to collect data and have 'legitimate interests' of the employer or a third party.

Employment Practices Code – www.ico.org.uk

The Code is issued by the Information Commissioner's Office (ICO) and sets out recommendations to help organisations comply with the law when carrying out monitoring. For example, unless exceptional circumstances apply (such as where a covert investigation can be justified) employees should be made aware that they may be monitored.

The Code provides criteria which employers are expected to meet in order to comply with the DPA. In any prosecution or enforcement proceedings, account will be taken of the employer's regard for these benchmarks, the first of which is for employers to: 'establish, document and communicate a policy on the use of electronic communications systems'.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 – www.legislation.gov.uk/uksi/2000/2699/contents/made

These Regulations provide for certain circumstances in which intrusive techniques can be used in the business context, for example:

- Preventing the unauthorised use of computer/telephone systems – ensuring the employee does not breach the organisation's email, internet or telephone policies.
- Preventing or detecting criminal activity.
- Maintaining the integrity of the organisation's systems (such as preventing viruses).
- Recording evidence of business transactions.

- Ensuring compliance with regulatory or self-regulatory guidelines.

The Code and the Regulations stipulate that the employer should take reasonable steps to inform employees in advance that their communications may be intercepted, and how information obtained from the monitoring may be used, for example a User Acceptance Policy or periodic communications to employees.

CCTV Code of Practice 2015 – https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

This Code provides good practice advice for those involved in operating CCTV and other surveillance camera devices that view or record individuals. It covers the use of camera related surveillance equipment including Automatic Number Plate Recognition, body worn video, and unmanned aerial vehicles (drones). The Code also provides guidance on information governance requirements, such as data retention and disposal.

Investigatory Powers Act 2016 (IPA) – https://www.gov.uk/government/collections/investigatory-powers-bill

IPA regulates the use of intrusive surveillance and investigation techniques, including the interception of communications (for example telephone calls or emails). It sets out legal requirements of when and how public authorities acquire, store and access information.

Employment Rights Act 1996 - https://www.legislation.gov.uk/ukpga/1996/18/contents.

The **Employment Rights Act** (ERA) **1996** set out the **rights** of **employees** in situations such as dismissal, unfair dismissal, parental leave, and redundancy.

ACAS Codes - https://www.acas.org.uk/codes-of-practice.

Acas codes of practice set the minimum standard of fairness that workplaces should follow. They are used by employment tribunals when deciding on relevant cases**.**

Appendix 2 – Security Investigation checklist

Step	Action	Comments	Complete
1	Does your organisation have security policies, available to all members of staff, which stipulate clearly what constitutes improper behaviour in the workplace, and what sanctions will be invoked if employees contravene these policies?		
2	Do employees have the means to communicate concerns about their colleagues?		
3	Have you prepared a scope and purpose document?		
4	Have you considered what factors may affect the investigation?		
5	Whom do you need to inform that a security investigation has been launched.		
6	Are you aware of the legal framework surrounding security investigations?		
7	Have you interviewed the source(s) of the reporting, all relevant witnesses and the employee under investigation covering Who, What, When, Why and How? Have written statements been prepared and signed by those interviewed?		
8	Is there a clear record of each stage of the security investigation?		
9	Is all monitoring compliant with relevant legislation?		
10	Have you prepared a concise and factual report to allow others to make a fair and balanced decision regarding the employee under investigation?		
11	Has a disciplinary hearing been held?		
12	Once the investigation is complete, is there scope for a review of the security investigation?		

Appendix 3 – An illustrative case study

The Security Manager of a large CNI utility company in the UK received a phone call on an emergency hotline outside of normal working hours from an employee (Mr A) working at a key site. Mr A reported he had found a security survey report containing vital information about security measures at the site but in an insecure location. The document contains the company logo and is marked as 'Company Confidential' with a restricted readership list.

The Security Manager confirmed the identity of Mr A and his contact details. Mr A was able to secure the document overnight and a member of the Security Team travelled to the site and recovered the document the following day. Upon sight of the document the Security Team were able to confirm that this was a security breach and plan how to conduct an investigation into the incident. A Senior Manager responsible for security was then briefed on the breach.

The Security Manger and a second member of the security team interviewed Mr A to confirm the circumstances of him finding the document (who, what, where, when and why). A full statement of the interview was produced and signed by both parties. Mr A was able to identify other potential witnesses.

The Security Manager briefed upwards to his Senior Manager, and they agreed to inform CPNI because the document, although not containing any protectively marked information, could allow interference of the workings of a key CNI site, impacting a variety of government and commercial customers.

The organisation's legal advisor was briefed on the circumstances of the breach. The Security Manager shared the investigation plan, and the legal advisor was able to confirm which staff policies would be relevant and advise on potential areas of legal concern for the organisation.

The Security Team began their investigations by interviewing all those who would logically have normal control of the document and gradually began to understand at what point the document became unsecured. The main concern for the investigators was the possibility that the document had been deliberately accessed by someone with malicious intent. Further investigations confirmed that this was not a malicious act, but poor security behaviours by a number of employees.

Disciplinary proceedings led to sanctions on those involved. The post investigation review revealed that all staff across the organisation required refresher training on secure document handling and that this needed to be repeated annually. The training staff had received on document handling was not consistent, often based on word of mouth from established staff, and this had allowed short cuts and poor practice to become the norm.

Mr A, who found the document and reported it immediately to the Security Department, received a gift voucher in recognition of his efforts.

The organisation ran the CPNI Workplace Behaviour Change Campaign and saw a reduction in security breaches and an increase in incident reporting.

Appendix 4 – Reporting concerns

Employers should offer their staff easy to use, non-confrontational and secure means of reporting concerns about colleagues and security matters in general. These measures should be advertised to staff and should be easily accessible e.g. on a company intranet site, staff notice boards and within induction materials. They can also be explained further during staff training or awareness events.

Methods of reporting include:

Line manager reporting

In organisations with a good security culture, the line manager will usually be the first point of contact for employees to report concerns about their colleagues such as failure to adhere to security procedures, bullying, fraud or theft. This may take place at either regular meetings, security appraisals or on an ad hoc basis.

Employee hotlines

These enable employees to report suspicions or actual incidents of illegal, improper or unethical conduct by colleagues, employers, clients or third parties. They can take the form of a dedicated telephone hotline, internet/intranet contact site, or a dedicated company email address. These hotlines are not intended to replace the line manager-employee relationship, but can provide additional benefits such as out-of-hours reporting, where desirable.

Employee hotlines can be anonymous. As far as possible, employers should provide assurances that anonymity will be preserved. In some cases, it may not be possible to carry out the entire investigation without revealing the employee's identity. Depending on the severity of the reporting, it may be necessary to consult the employee making the report should an investigation reach the point of having to reveal their identity.

Further information on reporting workplace behaviour of concern can be found in CPNI's It's Ok To Say programme.

Disclosures

Occasionally, officials from security authorities such as CPNI or law enforcement agencies may wish to speak to an employer about an employee. Typically, this will be to request information about an employee to help an ongoing investigation, however, this may not mean that the employee is engaged in any illegal activity. Further information on handling disclosures can be found in CPNI's *Managing the disclosure of employee-related information*.

Other sources of reporting

Other possible sources of reporting concerns include: speaking directly with security or HR departments (for example, by operating an 'open door' policy), workplace gossip, complaints from members of the public, or even acts of revenge by disgruntled friends or spouses. All sources of reporting must be assessed for relevance and accuracy.

Appendix 5 – Possible Data Sources for Security Investigation Analysis

Technical Data Sources

Account Creation Logs
Active Directory Logs
Antivirus Log
Application Logs
Authentication Logs
Chat Logs
Configuration Change Logs
Data Loss Prevention Logs
Domain Name System (DNS) Log
Email Logs
File Access Logs
Firewall Logs
Helpdesk Ticket System Logs
HTTP/SSL Proxy Logs
Intrusion Detection Prevention Logs
Mobile device Manager Logs
Network Monitoring Logs
Network Packet Logs
Permission Change Monitor Logs
Printer/Scanner/Copier/Fax Logs
Removable Media Manager Logs
VPN Logs
Wireless Spectrum Monitoring Logs

Non Technical Data Sources

Anonymous reporting lines
Asset Management Records
Acceptable User Policy Breach Records
Background Investigations
Corporate Credit Card Records
Conflict of Interest Reporting
Disciplinary Records
Foreign Contact and Travel Records
IP Policy Breach Records
Performance Appraisals
Personnel Records
Physical Access Records
Physical Security Breach Reporting
Security Clearance Records