Information Security Policy

Contents

Information Security Policy

1. **Purpose**
   1.1. This policy provides a framework for the management of information security throughout the organisation known as Psychometric Testing Solutions Insight (PTS Insight).
   1.2. It applies to: -
      1.2.1. all those with access to PTS information systems, including staff, visitors, and contractors.
      1.2.2. any systems attached to PTS computer or telephone networks and any systems supplied by PTS.
      1.2.3. all information (data) processed by PTS pursuant to its operational activities, regardless of whether it is processed electronically or in paper (hard copy) form,
      1.2.4. any communications sent to or from PTS and any information (data) held on systems external to PTS's network.
      1.2.5. all external parties that provide services to PTS in respect of information processing facilities and business activities; and principal information assets including the physical locations from which PTS operates.

2. **Aims and Commitments**
   2.1. PTS recognises the role of information security in ensuring that users have access to the information they require in order to carry out their work. Computer and information systems underpin all activities and are essential to its administrative functions and delivery of services.
   2.2. Any reduction in the confidentiality, integrity or availability of information could prevent PTS from functioning effectively and efficiently. In addition, the loss or unauthorised disclosure of information has the potential to damage PTS's reputation and cause financial loss. The Information Commissioner's Office (ICO) has the power to fine organisations for breaches of the Data Protection Act.
   2.3. To mitigate these risks, information security must be an integral part of information management, whether the information is held in electronic or hard-copy form.
   2.4. PTS is committed to protecting the security of its information and information systems in order to ensure that:
      2.4.1. the integrity of information is maintained, so that it is accurate, up to date and 'fit for purpose'.
      2.4.2. information is always available to those who need it and there is no disruption to the business of PTS.
      2.4.3. confidentiality is not breached, so that information is accessed only by those authorised to do so.
      2.4.4. PTS meets its legal requirements, including those applicable to personal data under the Data Protection Act; and
      2.4.5. the reputation of PTS is safeguarded.
   2.5. In order to meet these aims, PTS is committed to implementing security controls that conform to best practice.
   2.6. Information security risk assessments should be performed for all information systems on a regular basis in order to identify key information risks and determine the controls required to keep those risks within acceptable limits.
   2.7. PTS is committed to providing sufficient education and training to users to ensure they understand the importance of information security and, in particular, exercise appropriate care when handling confidential information.
   2.8. The Managing Partner shall advise on best practice and coordinate the implementation of information security controls.

2.9. PTS will establish and maintain appropriate contacts with other organisations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.
2.10. Breaches of information security must be recorded and reported to the Managing Partner will take action and inform the relevant authorities.
2.11. This Policy and all other supporting policy documents shall be communicated as necessary throughout PTS to meet its objectives and requirements.

3. Responsibilities

3.1. The Managing Partner has ultimate responsibility for information security within PTS. More specifically, he is responsible for ensuring that PTS complies with relevant external requirements, including legislation.
3.2. He is also responsible for:
3.2.1. ensuring that users are aware of this policy.
3.2.2. monitoring compliance.
3.2.3. conducting regular reviews of the policy, having regard to any relevant changes in legislation, organisational policies and contractual obligations; and
3.2.4. ensuring there is clear direction and visible management support for security initiatives.
3.2.5. All PTS staff.
3.2.6. All PTS staff are responsible for information security within their functions.
3.2.7. They must ensure they meet and are consistent with the requirements of the overarching policy.
3.3. They must address any queries on implementation of the policy to the Managing Partner.
3.4. Users and External Parties
3.5. Users of PTS information will be made aware of their own individual responsibilities for complying with PTS policies on information security.
3.6. Agreements with third parties involving accessing, processing, communicating, or managing PTS information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements.

4. Risk Assessment and the Classification of Information

4.1. Risk assessment of information held.
4.2. The degree of security control required depends on the sensitivity or criticality of the information. The first step in determining the appropriate level of security therefore is a process of risk assessment, in order to identify and classify the nature of the information held, the adverse consequences of security breaches and the likelihood of those consequences occurring.
4.3. The risk assessment should identify the PTS information assets; define the ownership of those assets; and classify them, according to their sensitivity and/or criticality to PTS. In assessing risk, PTS should consider the value of the asset, the threats to that asset and its vulnerability.
4.4. Where appropriate, information assets should be labelled and handled in accordance with their criticality and sensitivity.
4.5. Rules for the acceptable use of information assets should be identified, documented and implemented.
4.6. Information security risk assessments should be repeated periodically and carried out as required during the operational delivery and maintenance of the PTS infrastructure, systems and processes.
4.7. Personal Data
4.7.1. Personal data must be handled in accordance with the Data Protection Act 1998 (DPA) and in accordance with the PTS Data Protection Policy.

4.7.2. The DPA requires that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

4.7.3. A higher level of security should be provided for 'sensitive personal data', which is defined in the DPA as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership, or the commission or alleged commission of criminal offences.

5. Protection of Information Systems and Assets

5.1. It is an essential part of our data protection process that all staff and others who come into contact with our systems and assets have been trained in data security and also sign a confidentiality agreement and that by doing so understands that they are bound by the information classification of OFFICIAL under the 2014 United Kingdom information classification protocol.

5.2. As in 5.1 the treatment of all assets such as any issued equipment i.e. Laptop Computers, Mobile telephones or any other asset deemed to be within the scope of the protocol

5.3. Confidential information should be handled in accordance with the requirements set out in section 6 below.

6. Protection of Confidential Information

6.1. Identifying confidential information is a matter for assessment in each individual case. Broadly, however, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences: -

6.1.1. Financial loss

6.1.2. Reputational damage

6.1.3. An adverse effect on the safety or well-being of members of PTS or those associated with PTS.

7. Storage

7.1. Confidential information should be kept secure, using, where practicable, dedicated storage (e.g., file servers) rather than local hard disks, and an appropriate level of physical security.

7.2. File or disk encryption should be considered as an additional layer of defence, where physical security is considered insufficient.

8. Access

8.1. Confidential information must be stored in such a way as to ensure that only authorised persons can access it.

8.2. All users must be authenticated. Authentication should be appropriate, and where passwords are used, clearly defined policies should be in place and implemented. Users must follow good security practices in the selection and use of passwords.

8.3. Where necessary, additional methods of authentication should be considered.

8.4. To allow for potential investigations, access records should be kept for a minimum of six months, or for longer, where considered appropriate.

8.5. Users with access to confidential information should be security vetted, as appropriate, in accordance with existing policies.

8.6. Physical access should be monitored, and access records maintained.

9. Remote access

9.1. Where remote access is required, this must be controlled via a well-defined access control policy and tight access controls provided to allow the minimum access necessary.

9.2. Any remote access must be controlled by secure access control protocols using appropriate levels of encryption and authentication.

10. Copying

10.1. The number of copies made of confidential information, whether on portable devices or media or in hard copy, should be the minimum required, and, where necessary, a record kept of their distribution. When no longer needed, the copy should be deleted or, in the case of hard copies, destroyed.

10.2. All copies should be physically secured e.g. stored in a locked cupboard drawer or filing cabinet.

11. Disposal

11.1. Policies and procedures must be in place for the secure disposal/destruction of confidential information The PTS disposal of old computers is supervised by the Managing Partner and involves total destruction to standard procedures.

12. Use of portable devices or media

12.1. Procedures should be in place for the management of removable media in order to ensure that they are appropriately protected from unauthorised access.

12.2. The permission of the information owner should be sought before confidential information is taken off site. The owner must be satisfied that the removal is necessary and that appropriate safeguards are in place e.g., encryption.

12.3. In the case of personal data, the ICO recommends that all portable devices and media should be encrypted where the loss of the data could cause damage or distress to individuals.

12.4. The passphrase of an encrypted device must not be stored with the device to ensure that data are appropriately secured and that all legal and regulatory requirements have been considered.

13. Exchange of Information and use of email

13.1. Controls should be implemented to ensure that electronic messaging is suitably protected.

13.2. Email should be appropriately protected from unauthorised use and access.

13.3. Email should only be used to send confidential information where the recipient is trusted, the information owner has given their permission, and appropriate safeguards have been taken e.g., encryption.

14. System planning and acceptance.

14.1. A risk assessment should be carried out as part of the business case for any new ICT system that may be used to store confidential information. The risk assessment should be repeated periodically on any existing systems.

15. Backup

15.1. Information owners should ensure that appropriate backup and system recovery procedures are in place. Backup copies of all important information assets should be taken and tested regularly in accordance with such an appropriate backup policy.

16. Hard Copies

16.1. Protective marking

16.1.1. Documents containing confidential information should be marked as ‘Confidential’ or with another appropriate designation e.g., ‘sensitive’, etc., depending on the classification system adopted by the department.

16.2. Storage

16.2.1. Wherever practicable, documents with confidential information should be stored in locked cupboards, drawers, or cabinets. Where this is not practicable, and the information is kept on open shelving, the room should be locked when unoccupied for any significant length of time.

16.2.2. Keys to cupboards, drawers or cabinets should not be left on open display when the room is unoccupied.

16.3. Removal

16.3.1. Confidential information should not be removed from PTS unless it can be returned on the same day or stored securely overnight, as described in the section above.

16.4. Transmission

16.4.1. If confidential documents are sent by fax, the sender should ensure they use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

16.4.2. If confidential documents are sent by external post, they should ideally be sent by a form of recorded delivery. The sender must ensure that the envelope is properly secured.

16.4.3. If confidential documents are sent by internal post the documents should be placed in an envelope marked 'Confidential' with the addressee's name clearly written on it.

16.5. Disposal

16.5.1. Confidential documents must be shredded in a confidential manner prior to disposal and in accordance with BS EN 15713

16.6. Enforcement

16.6.1. There must be a written policy in place for the handling of confidential information, whether electronic or hard copy and a copy of the procedures must be provided to every user so that they are aware of their responsibilities.

16.6.2. Any failure to comply with the policy may result in disciplinary action.

16.6.3. Any loss or unauthorised disclosure must be promptly reported to the owner of the information.

16.6.4. Computer security incidents involving the loss or unauthorised disclosure of confidential information held in electronic form must be reported to the Managing Partner and investigated.

16.6.5. If the loss or unauthorised disclosure involves personal data, whether electronic or hard copy, the Managing Partner must be informed.

17. Compliance

17.1. PTS has established this policy to promote information security and compliance with relevant legislation, including the DPA. PTS regards any breach of information security requirements as a serious matter, which may result in disciplinary action.

17.2. Compliance with this policy should form part of any contract with a third party that may involve access to network or computer systems or data.

17.3. Relevant legislation includes, but is not limited to:-

17.3.1. The Computer Misuse Act (1990)

17.3.2. The Data Protection Act (1998)

17.3.3. The Regulation of Investigatory Powers Act (2000)

17.3.4. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)

18. Other Relevant PTS Policies or Guidance

18.1. Data Protection Policy

18.2. Confidentiality Policy

18.3. Document and Records Management Policy

18.4. Information Sharing Policy

19. Glossary

Access Control - ensures that resources are only granted to those users who are entitled to them.

Appropriate - suitable for the level of risk identified and justifiable by risk assessment.

Asset – anything that has a value to PTS.

Audit - information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

Authentication - the process of confirming the correctness of a claimed identity.

Best Practice – current standard advice for implementing security controls. Synonymous with 'good practice'.

Confidentiality - Confidentiality is the need to ensure that information is disclosed only to those who are authorised to view it.

Control – a means of managing risk by providing safeguards. This includes policies, procedures, guidelines, other administrative controls, technical controls or management controls.

Data - Information held in electronic or hard copy form.

DPA – Data Protection Act 1998

External Party - see 'Third Party'.

ICO – Information Commissioner's Office (http://www.ico.gov.uk/)

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual.

Information Owner – synonymous with 'information risk owner'. This is the person who is responsible for accepting any residual risk.

Information Security – Preservation of confidentiality, integrity and availability

Information Systems – Any system, service or infrastructure used to process information or the physical locations housing them. This includes critical business environments, business processes, business applications (including those under development), computer systems and networks.

Personal Data – Any data held in a system, whether electronic or hard copy, that identifies a living individual (for a legal definition, see Data Protection Act 1998).

Policy – overall intention and direction as formally expressed by management.

Protocol – Any other existing system of governance

Risk - the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities

Risk Assessment – overall process of identifying and evaluating risk.

Third party – person or body that is recognised as being independent of PTS

Threat – something that has the potential to exploit a weakness to result in some form of damage. Threats can be environmental, deliberate, accidental, logical or technical.

Vulnerability – weakness of an asset or group of assets that may be exploited by a threat.