IDENTITY

,

Information Security Policy

Identity Events Management – Sole Proprietorship LLC

Version 001 dated: 01/03/2023

March 2023

BACKGROUND

This Policy applies to all Members and employees of Identity, both permanent and temporary. It also applies to contractors, business partners and visitors, not employed by Identity but engaged to work with or who have access to Identity information, (e.g., computer maintenance contractors) and in respect of any externally hosted computer systems.

Suitable third-party processing agreements must be in place before any third party is allowed access to personal information for which Identity is responsible.

PURPOSE

The policy ensures that the organisation minimises risks associated with the loss of Confidentiality, Integrity and Availability (CIA):

- Confidentiality - accidental or malicious disclosure of information
- Integrity - accidental or malicious modification of information
- Availability - information not available to those who need it

SCOPE

The Policy applies to all locations from which Identity's systems are accessed (including home use). Where there are links to enable third-party organisations to have access to Identity information, managers must confirm the security policies they operate meet Identity's security requirements. A copy of any relevant third-party security policy should be obtained and retained with the contract or agreement.

Policy continues overleaf.

INFORMATION SECURITY POLICIES

All staff must be aware of and understand the content of this policy.

Team Leaders should be aware of the following topic-specific control policies and documents, which further mandate the implementation of information security controls:

Policy	Owner
IS Policy Statement	IT Manager
Acceptable Use Policy	IT Manager
Remote Working Policy	IT Manager
Data Protection Policy	IT Manager
Systems Development Policy	IT Manager

RESPONSIBILITIES FOR INFORMATION SECURITY

All Staff are responsible for:

- ensuring that no breaches of information security result from their actions
- reporting any breach, or suspected breach of security without delay. Further details can be found in the Security Incident and Personal Data Breach Policy
- reporting any outage of services without delay.
- ensuring information, they have access to remains secure. The level of security will depend on the sensitivity of the information and any risks which may arise from its loss.

Advice and guidance on information security can be provided by the IT Manager.

HUMAN RESOURCE SECURITY

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

1. All staff should be aware of the confidentiality clauses in their contract of employment.

2. All Staff should attend induction training on Information Security.

3. If any user is found to have breached this policy, they could be subject to the organisation’s Disciplinary and Dismissal Policy & Procedure. Serious breaches of this policy could be regarded as gross misconduct.

ASSET MANAGEMENT

Objective - To ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.

4. All staff should be aware of the Acceptable Use Policy and the rules associated with information assets and information processing facilities.

5. All employees and external party users shall return all of the organisational assets in their possession upon termination of their employment, contract or agreement.

6. All staff should be aware of the Data Classification, Information Labelling and Handling Procedures, which ensure that information is protected at an appropriate level.

7. The use of personal USB drives is not permitted. Only authorised company encrypted removable media shall be used, with express authorisation from the Data and Security Manager who will ensure appropriate security controls have been implemented.

ACCESS CONTROL

Objective: To limit access to information and information processing facilities

8. Staff and contractors should only access systems for which they are authorised. Do not attempt to gain access to computer information and systems for which they have no authorisation.

9. Staff and contractors must comply with the organisation's requirements for passwords, which is outlined in the Acceptable Use Policy for the concerned person's team.

10. Passwords must be changed if a user suspects that their password may have been compromised.

PHYSICAL AND ENVIRONMENTAL SECURITY

Objective: To prevent unauthorized physical access, damage and interference to the organisation's information and information processing facilities.

11. All staff members must ensure their visitors sign the Visitors book and provide identification as required.

12. Staff should accompany visitors within any rooms that may contain confidential the organisation data or data from the organisation's customers. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

13. Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas. Staff should not let someone in they do not know or recognize nor allow anyone to tailgate them through security doors.

Clear Desk Policy

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

14. Staff are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers and cupboards as appropriate.

15. Any Restricted or Sensitive information must be removed from the desk and locked in a locked drawer or cabinet when the desk is unoccupied and at the end of the work day.

16. Although security measures are in place to ensure only authorised access to office areas, staff should ensure that documents, particularly of a confidential nature are not left lying in open view.

17. Passwords must not be written down or left in an accessible location.

18. Printouts containing Restricted or Sensitive information should be immediately removed from the printer.

19. Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins.

20. Staff must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

Security of Equipment

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

21. Staff should not leave their computers unlocked and unattended.

22. Staff should ensure that all Computers assigned to them are configured to auto-lock the screen after 5 minutes of inactivity.

23. As computer equipment is vulnerable to theft, loss or unauthorised access, staff must always secure laptops and handheld equipment when leaving an office unattended and lock equipment away.

24. Due to the high incidence of car thefts, staff should not leave laptops or other portable equipment unattended in cars or take them into vulnerable areas.

25. Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off the organisation property. The equipment should only be used by the individual to which it is issued.

26. Staff working from home must ensure appropriate security is in place to protect the organisation equipment or information. This will include physical security measures to prevent unauthorised entry to the home and ensuring the organisation equipment and information is kept out of sight.

27. the organisation issued equipment must not be used by non-the organisation staff.

28. Users of this equipment must pay particular attention to the protection of personal data and commercially sensitive data. The use of a password to start work with the computer when it is switched on, known as a 'power on' password, is mandatory and all sensitive files must be encrypted at rest and in transit.

29. Staff who use computers belonging to the organisation must use them solely for business.

30. If any team member loses a company computer or device they must notify their Team Lead and the IT Manager as soon as possible – lost or stolen devices may result in a data breach.

Working in Secure Areas

Objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.

31. For all employees, third parties and other stakeholders who are given access to a secure area the following procedural instructions will apply.
    - Ensure you understand the specific instructions for all secure areas to which you are granted access.
    - Don't tell anyone about the secure area if you are requested not to.
    - Inform security of visitors that you are expecting in plenty of time and escort your visitors at all times.
    - Don't keep secure doors open for longer than necessary and never allow anyone to tail-gate behind you through a secure entry point.
    - No employees should work in the secure area on their own unless by prior arrangement.
    - Never lend anyone your access keys or expose it to possible theft or loss. Challenge and/or report anyone not wearing a visitor badge and remain vigilant whilst within the secure area.

- Check vacant areas for signs of unauthorised access and always ensure that doors and windows are secure before leaving if you are the last one out of the secure area.
- The use of photographic, video or audio recording equipment is prohibited within the secure area unless by prior arrangement with security.
- Do not leave classified information unattended in clear view of visitors.

COMMUNICATIONS SECURITY

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

32. If information is particularly sensitive or confidential then staff must consider the most secure method of transmission.

33. Staff should not use email to communicate internally with other members of the organisation staff; staff should use secure, encrypted communication methods such as Teams

34. Customer data should never be shared internally via email, or any other medium except by sharing via the organisation's SharePoint or Teams

35. When sending information by email to external parties, staff should:
    - Carefully check the recipient's email address before pressing send – this is particularly important where the 'to' field autocompletes
    - Not send sensitive information via email, rather, staff may email to external parties a sharable link to a OneDrive file (this is both secure and auditable)
    - Take care when replying 'to all' and ensure that one is aware of all recipients, taking note of any mailing list addresses
    - Consider the use of secure email where this is available, or use drop off and encrypt the document
    - Not send any the organisation or customer files to a user's personal mailbox.

36. When disclosing personal or sensitive information to customers, particularly over the phone or in person, staff should verify their identity of the person with whom they are speaking. If in doubt, ask for suitable ID or offer to post the information (to the contact details you have on file).

37. If a request for disclosure of information is received from a third party, staff must:
    - Obtain written consent from the customer that they are acting on their behalf
    - verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation. Do not take their mobile number and use that.

38. In all circumstances, staff must ensure that they are legally able to share the information being requested and only share the minimum amount of information necessary.

OPERATIONS SECURITY

Objective: To ensure correct and secure operations of information processing facilities.

39. Staff are forbidden to use personal cloud storage solutions or personal email accounts to conduct the organisation business or store any work-related files.

40. Staff should not use any cloud service – for storage or otherwise – not explicitly approved by the IT Manager, nor should staff use the organisation email accounts to sign up for such unapproved services nor may they use the organisation machines to log into such unapproved services. A list of approved services is maintained by the IT Manager.

41. Users are responsible for ensuring that their computers or mobile devices receive all security updates from the operating system distributor or manufacturer. It is a considerable risk to not install security updates.

42. Users are responsible for checking that virus updates are automatically occurring on all desktop machines. Any suspected virus attacks must be reported to the respective manager.

SOFTWARE

Objective: To ensure the integrity of operational systems

43. All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

44. The loading and use of unlicensed software on the organisation computing equipment is strictly prohibited. The organisation monitors the installation and use of software by means of randomised software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the organisation's Disciplinary and Dismissal Policy & Procedure.

45. the organisation will only permit authorised software to be installed on its PCs.

46. Software packages must comply with and not compromise the organisation's security standards.

47. Computers owned by the organisation are only to be used for the work of the organisation. The copying of leisure software on to computing equipment owned by the organisation is not allowed. Copying of leisure software may result in disciplinary action under the organisation's Disciplinary and Dismissal Policy & Procedure. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

End of policy.