Network Security

What are system security procedures?

Example of a policy detailing the methods and guidelines regarding the operating system and server security in an organisation. It may also include training, procedures and the importance of computer security system

For more information https://spscc.edu/policy/pritsv4702

Examples of security features of network can include:

- Virus scanning
- Individual logging in
- Administrator accounts
- Automatic logging out
- Server has admin access only
- Server back up
- Administrator accounts
- OS regularly updated
- Locked features where necessary (such as educational institutions limiting access to the control panel)

Physical security:

- Cameras
- locked down equipment
- security doors
- swipe card access
-

Network Security - Protective Security Policy Framework

Mandatory

https://www.protectivesecurity.gov.au/overarching-guidance/Pages/Mandatory-requirements.aspx broken link – search: https://www.protectivesecurity.gov.au/Pages/default.aspx

Storage and security of personal information

Consider how technology has altered the way information is now collected and stored digitally. The ethics and privacy laws regarding online data storage (for example) had to be created by governments which were then implemented and filtered through to each organization and then to its employees.

The education of the rights, obligations and responsibilities for each staff member is therefore very important and essential to the successful running of a business.

Prevention of internal and external threats by:

- regularly assessing the risk of misuse, interference, loss, and unauthorised access, modification or disclosure of that information
- taking measures to address those risks, for example, keep a record (audit trail) of when someone has added, changed or deleted personal information held in our electronic databases and regularly check that staff only access those records when they need to
- conduct regular internal and external audits to assess whether we have adequately complied with or implemented these measures
- Use of Encryption
- Destroy personal information in a secure manner when no longer needed. For example, destroy complaint records after two years, in accordance with the OAIC's Records Disposal Authority.