WSY
PUBLISHING
• EST 1887 •

Information Technology Security Policy

This policy should be read and carried out by all WSY staff.

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the business to ensure integrity, confidentiality and availability of data and assets. Information security is the responsibility of all employees. Any employee becoming aware of a breach to any security requirement is obliged to notify (insert name: the CIO?) immediately.

Physical Security

All security and safety of all technology, such as laptops and desk computers, will be the responsibility of the employee who has been issued with the asset. Each employee is required to use passwords and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, (insert name: CIO?) will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

Bring Your Own Device:

Employees can bring their own devices to the office.

However, they must not connect their personal devices to the company's networks and systems.

Employees must not conduct any business-related activity on their private device. Employees must use the computer/devices they are provided for any work-related activity.

WSY
PUBLISHING
• EST 1887 •

Information Security

All important information, such as sensitive, valuable, or critical business data, is to be backed-up.

It is the responsibility of each employee to ensure that data back-ups are conducted at the end of every business day, and the backed-up data is kept on a separate hard drive protected by password.

All technology that has internet access must have anti-virus software installed. It is the responsibility of (who – CIO?) to install all anti-virus software and ensure that this software remains up to date on all technology used by the business.

All information used within the business is to adhere to the privacy laws and the business's confidentiality requirements. Any employee breaching this will be subjected to disciplinary measures, including possible termination.

Technology Usage and Management

Every employee will be required to set a password for access to all devices.

Each password must be changed every two weeks.

Each password is to be at least 20 characters in length, and include the following:

- No common names or dictionary words
- No sequences of more than 4 digits in a row
- Include at least one character from at least 3 of these categories:
- Uppercase letter
- Lowercase letter
- Digits
- Special character

Passwords must not be shared with any employee within the business.

Employees are only authorised to use business computers for personal use during break times.

For internet and social media usage, refer to the Human Resources Manual.

Source:

This document was produced by UNSW Online using a publicly available template created by the State Government of Victoria. Original template available here:

https://business.vic.gov.au/tools-and-templates