WSRC Information Security Policy

Introduction

The objective of this policy is to protect the confidentiality, integrity and availability of information and information systems under our control. To this end, we will:

- Protect the organisation's people and property
- Protect our members' information and property
- Comply with all relevant laws and regulations
- Fulfil or exceed our contractual obligations
- Educate employees on their responsibilities
- Report security incidents and concerns immediately

Policy

- An accurate inventory of information assets shall be maintained.
- Access to information facilities, systems and networks shall be limited to authorised users.
- Privileged access rights will be restricted to qualified staff on a need-to-know basis.
- Use of information systems shall be for legitimate business purposes only.
- Passwords must be complex and must not be disclosed or shared.
- Equipment shall be protected from loss, damage and theft.
- Antivirus software shall be operational and up to date.
- Firewalls shall be enabled with approved rules.
- Wireless access must be secured with WPA2 and/or VPN.
- Software security patches will be installed as soon as possible.
- Backups will be maintained and tested regularly.
- The processing of personal data shall be controlled and documented.
- Confidential information must not be disclosed without authorisation.
- Confidential information must be adequately protected during transit and storage.
- Use of information systems and networks will be routinely logged and monitored.
- Security requirements will be established and agreed with relevant parties.
- Security incidents and concerns must be reported immediately.
- Employees shall be subject to disciplinary action for non-compliance.