6.8 Network Security Policy

Intent

The employer strives to protect company computer networks from both internal and external threats to their integrity, and to preserve confidentiality. This policy has been adopted to ensure that every reasonable effort has been taken to prevent and mitigate the effects of serious risks and potential costs associated with threats to networks and network resources.

Scope

This policy applies to all employees always and without exception.

Unionized employees are requested to refer to their current Collective Agreement for specific information pertaining to network security. Where a Collective Agreement is silent on the issue, this policy shall dictate the requirements for unionized employees. In situations where the directions of this policy cover issues also in the Collective Agreement, the Collective Agreement will be the final authority.

Guidelines

Threats to the security of computer networks pose a significant risk to the organization's ability to carry out its operations.

The network operates at the continual risk of intrusions such as, but not limited to, theft of confidential information, the spread of viruses and malware and other activities designed to damage and or destroy network functionality.

The employer has an obligation to exercise due diligence to protect sensitive data and may face legal action if personal and or confidential information is disclosed.

Network Users:

- Comply with all employer policies.
- Comply with all protocols regarding connection to company networks.

IT Department or Representative:

- Act as the final authority on all network security related activities.
- Oversee any investigations into alleged network security issues.
- Develop protocols for tracking suspected network intrusions and test these methods for validity.
- Work with appropriate authorities towards the identification and prosecution of groups and individuals involved in activities in violation of company policy and the law.
- Post security alerts, network usage best practices and any other information required to protect the network.
- Monitor all network traffic to detect any unauthorized activity, attempts at intrusion and compromised hardware in compliance with privacy and confidentiality policies.
- Resolve any identified potential or actual problems in collaboration with appropriate managers.
- Regularly test the network for vulnerabilities using appropriate tools.
- Report any ongoing concerns to management.

- Undertake any necessary upgrades and or repairs to the network to maintain network security.
- Produce quarterly reports of all security related activities, concerns and or problems identified and resolved.
- IT Department or representative contact information should be posted in all departments.