Information Systems Security

Information Systems
Policy R3

Policy:	R3 – Information Systems Security
Policy Department(s):	Information Systems
Adoption Date:	January 27, 2025
Adoption Reference:	CM20250127.016
Effective Date:	January 27, 2025
Last Amended:	N/A

Policy Purpose

To support the activities and procedures which are necessary to protect the County's technology and information assets from system failure and malicious intent, reduce the risk of Incidents occurring and minimize the operational impact of Incidents which occur.

Policy Statement

The County relies on technology to function operationally, provide services to residents and comply with legislation. Administration is committed to the security, stability and integrity of the County's technology resources, including but not limited to hardware, software, networks, business systems, cloud-based services, mobile devices, communications systems, removeable media, peripheral devices and data, either owned by the County or used for County business.

Definitions

"Cybersecurity Team" means the Information Systems staff responsible for managing, implementing, and administering the County's cybersecurity program, controls and policies.

"Disaster" means a sudden, unplanned event that causes significant damage or serious loss to an organization's IT systems or services, requiring disaster recovery efforts.

"Employee" means any person employed by the County of Grande Prairie on a permanent, temporary, seasonal, full-time, part-time or casual basis including all unionized, non-unionized and management staff.

"Incident" means an unplanned interruption to a service, or reduction in the quality of a service.

"Security Awareness Training" refers to the base set of educational courses or modules which enable Users to identify cybersecurity threats and how to handle them.

"Simulated Phishing Attacks" mimic real-world phishing attempts and give users the opportunity to practice identifying and reporting phishing emails.

"Technology Resources" includes, but is not limited to, hardware, software, networks, network infrastructure, data (information), data centers, databases, business systems, cloud-based

services, mobile devices, communications systems, removable media, peripheral devices and data, either owned by the County or used for County business.

“Technology Resource Users (Users)” means anyone who is authorized to use Technology Resources, including but not limited to Council Members, Employees, vendors, contractors, and consultants.

“Unacceptable Risk” means an uncertain event or condition, which if it occurs, has an unacceptable negative effect.

“Vulnerability” means a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Policy Guidelines

1. Technology Resources shall be safeguarded from malicious intent and Information shall be protected from unauthorized disclosure.
2. Technology Resources shall only be accessed by authorized Users for legitimate business purposes and used in an acceptable manner.
3. Users must be competent and proficient in the safe and secure use of Technology Resources, supported by training and ongoing education.
4. All Users must successfully complete recurring Security Awareness Training, be subject to Simulated Phishing Attacks and successfully complete training assignments from the Cybersecurity Team.
5. All hardware, software and business systems, including cloud-based services, must be authorized by Information Systems prior to purchasing or use for County business.
6. Technology Resources are selected and configured for optimum security, data integrity and privacy in compliance with current privacy legislation and industry standards.
7. Vulnerabilities and Unacceptable Risks are actively identified and resolved or mitigated.
8. The County shall be prepared to respond to Incidents in a timely and coordinated manner and to return to normal operations after a Disaster has occurred.

Attachments

N/A

References

Legal Authorities	Freedom of Information and Protection of Privacy Act
Related Plans, Bylaws, Policies, Etc.	Policy B1 – Policy Development
Other	Procedure R3 – Simulated Phishing Program Procedure R3 – Acceptable Use of Technology Resources

Revision History

Review Date	Description
January 27, 2025	Adoption Date CM20250127.016