P O L I C Y

Department Administration	Policy No. AD(44)	Page 1 of 6
Policy Title Cyber Security	Date:	Resolution No. C//21

Policy Purpose:

Lacombe County is committed to achieving a targeted level of protection from internal and external cyber security threats, and accordingly, will implement ongoing governance, policies, and practices which address the following objectives:

- Establish controls for protecting Lacombe County's information and information systems against theft, abuse, and other forms of harm or loss.
- Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach.
- Comply with requirements to ensure the confidentiality, integrity, and availability of County I.T. systems and assets for Lacombe County's employees, contractors, vendors, and other users.
- Motivate administrators and employees to maintain the responsibility for, ownership of, and knowledge about cyber security.
- Ensure the protection of Lacombe County's data and information assets.
- Ensure the availability and reliability of the network infrastructure, hardware, software systems and services.
- Ensure that external service providers are made aware of, and comply with, Lacombe County's cyber security needs and requirements and continuously assess whether they maintain an acceptable cyber security posture.
- Balance the need for the above with the investment and policy constraints required to achieve an appropriate level of protection while maintaining organizational agility.

Policy Scope:

This policy applies to all Lacombe County (hereinafter referred to as the "County") officials, employees, guests and third parties including all independent contractors, consultants, vendors, suppliers, agents, and other users of Lacombe County's I.T. resources (together referred to as "users") wherever they may be located. The policy is structured in the following categories:

A. Leadership and Governance
B. Access and Use
C. Operational Technology Requirements
D. Awareness and Training
E. Business Continuity
F. Disaster Recovery Plan

Policy Details:

A. Leadership and Governance

Cyber security is a strategic business matter for Lacombe County and is not just a technical consideration. The assessment and management of cyber risk involves both the County as a whole and each business unit. Accordingly:

- The development and endorsement of a cyber security plan at Lacombe County is the responsibility of the County Manager.
- The implementation of the cyber security plan and oversight of its effectiveness is the responsibility of the Manager of I.T. Services.
- Cyber risk will be reflected in reports and updates to senior management and Council on an annual basis.
- Cyber risk should become a standard consideration by all levels of staff where changes to business processes take place, which includes but is not limited to, the Information Technology environment.

B. Access and Use

Authorized use: Lacombe County provides access to I.T. resources to users in order to perform their roles for Lacombe County. Lacombe County prohibits use of I.T. resources for any purpose other than business, unless otherwise stated in this policy. All users must behave honestly with vigilance, respect the intended business use of technologies, and comply with software licenses, property rights, user agreements, confidentiality, and legal rights.

Limited personal use is acceptable provided that it does not affect job performance, is not for personal financial, commercial, or third-party gain, and if the user adheres strictly to this policy. Lacombe County systems must not be used for the creation or distribution of any material considered inappropriate, offensive, threatening, abusive, defamatory, unlawful, sexually explicit, sexist, racist, discriminatory, embarrassing, fraudulent or disrespectful to others or that could harm the reputation of the County and potentially breach any corresponding software licensing agreements. Lacombe County restricts all users from using the Internet to perform any task contrary to the law or knowingly accessing websites with content that is illegal, obscene, hateful, defamatory, indecent, objectionable, or inappropriate.

To maintain the integrity of Lacombe County's corporate image and reputation and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential, or personal information, employees must exercise caution and care when using any system, service, or technology platform, both internal and external, including email or third-party services, such as cloud-based services and social media platforms. Personally identifiable information (PII), which is any data that could identify a specific individual, should not be transmitted via email, or shared using any other service without prior approval by the County Manager or their respective Department Director. Employees must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

In addition to this policy, users are also bound by the County's Internet and Email Use Policy, AD(23) as well as Social Media Policies AD(42) and AD(43).

Active Directory Accounts: Internal accounts used by Lacombe County personnel must have a unique user ID and password which cannot be used by or shared with anyone other than for whom it is intended. Personnel external to Lacombe County (i.e., consultants and/or contractors) will be provided with unique user IDs and passwords, and follow the same internal controls relating to the granting and/or revoking of access as internal Lacombe County accounts. Contractors, vendors and/or consultants must ensure all accounts/passwords assigned to them remain confidential.

Active Directory constitutes the official corporate directory of users, and it must reflect up to date information, including but not limited to, user's full name, department, or functional area the user is associated with, direct reports, phone numbers, organizational position, or role, etc. It is the responsibility of every Department Director, or their assigned designate, to ensure the information is current by advising the I.T. Department of any change. Upon a change in a staff member's status, including promotion, transfer or termination of employment, the Human Resources will advise the Manager of I.T. Services of this change so that the employee's network and physical access privileges are modified as appropriate in a timely manner.

Passwords: Users are responsible for utilizing effective passwords as outlined in Administrative Directive CS (5) and for keeping those passwords secret and secure. Employees must not share, use, or disclose someone else's login or password without prior authorization by the employee's Department Director or Human Resources. The I.T. Department will support the mechanisms that evaluate the strength of passwords and, if warranted, define the password change frequency for every type of applications, services and devices supported by the County, along with other mechanisms to strengthen the way users identify themselves when accessing Lacombe County's I.T. resources, such as multifactor authentication. The I.T. Department will ensure there is a limit imposed on consecutively invalid login attempts and should that limit be reached, the specific user account will be locked until released by an administrator.

Multifactor Authentication: Multifactor Authentication (MFA) is a security feature offered by a growing number of applications, websites and devices that dramatically improves account security. Rather than just asking for a username and password, MFA requires one or more additional verification factors to sign into an account, enter a Virtual Private Network (VPN) or access an application. Usernames and passwords are important; however, they are one of the most vulnerable attack vectors used by cyber criminals and MFA provides a layered defense against unauthorized user access to the County's I.T. infrastructure. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the additional authentication requirement and will not be able to gain their desired access. The County will be enforcing MFA where it is available and deemed to be suitable. All cloud-based administrative accounts must implement MFA and must use different passwords than those used within the County's internal I.T. infrastructure.

Third Parties: Prior to any third parties, vendors, suppliers, partners, contractors, service providers, or customers being granted access to Lacombe County's internal network or access to Lacombe County's data, they will be provided a copy of this policy and must comply with all relevant components contained in the policy.

C. <u>Operational Technology Requirements</u>

Firewall: A firewall is a program or hardware appliance that monitors and analyzes the incoming and outgoing network traffic in the County's I.T. environment. The County has implemented a next-generation firewall that acts as the first line of security defense that protects the County's internal network from unauthorized outside intrusions. The County's firewall has also been configured to enable content filtering that limits certain categories of websites accessible from inside our network.

Security Software: Lacombe County has enabled security software to protect the organization's workstations and servers against threats of both known malware (viruses, worms, ransomware, and spyware) and zero-day threats. A zero-day threat is a vulnerability exploited by attackers before the vulnerability can be patched by the hardware, software, or programming vendor. The County's security software is configured to perform automatic updates of the software while also performing automated scans on a regular basis to ensure County devices remain up to date.

System Patching: Vendors constantly release software and firmware updates, otherwise known as patches, to address defects and security vulnerabilities in their products. The County uses a tool from Microsoft to check for these patches and download them to an update server. The I.T. Department will apply these patches on the County's servers on a weekly basis to ensure they remain up-to-date and free of known vulnerabilities. Patching of individual workstations, laptops and tablets is a responsibility of our staff. Each user must check for available updates on their devices on a weekly basis and install any available updates to ensure their devices remain up-to-date and free of known vulnerabilities.

***Email Security*:** Protecting email systems is a high priority as emails can lead to Phishing attacks, data theft, scams and carry malicious software in the form of viruses, spyware, Trojans, and other malware. As such, Lacombe County requires users to:

- Verify the legitimacy of each email, including inspecting the email address and sender name.
- Avoid opening suspicious emails, attachments and clicking on links.
- Look for significant grammatical errors.
- Avoid clickbait titles and links.
- Not send email messages containing unusually sensitive information over the Internet without using an encryption method approved by the County.
- Contact the I.T. Department if they receive suspicious looking emails.

***Transferring Data*:** Lacombe County recognizes the security risks of transferring corporate data both internally and externally. To minimize the chances of data loss and data theft, users must:

- Obtain the necessary authorization from the appropriate Department Director to transfer data outside the organization.
- Verify the recipient of the information and ensure they have the appropriate security measures in place on their end.

- Only use approved file transfer services for the uploading or sharing of County data to or from the cloud. Users are to coordinate with the I.T. Department to select these file transfer services to ensure they are secure and appropriate.
- Utilize secure portable media such as encrypted USB flash drives if they are transferring data between devices without using the cloud. The I.T. Department will supply these drives if needed.

Remote Access: Access to the County's data, system and network resources must be protected from unauthorized use that could lead to damaging attacks. While measures have been taken to enable working from a remote location, remote access is inherently a security risk to the organization. As such, Administrative Directive CS(5) has been implemented to manage this risk.

D. Awareness and Training

Human error remains the most common cause of cyber security incidents. As a first line of defense, the County's I.T. Department will provide an ongoing program for staff awareness and training as it relates to cyber security to ensure that clear cyber security expectations are set while also educating users on how to recognize attack methods, how to prevent cyber incidents and how to respond to potential threats. Cyber criminals are not only exploiting vulnerabilities in technology, but they also exploit people's behaviors and emotions. Developing a strong cyber security culture at Lacombe County will go a long way to reducing cyber risk for our organization.

New Employees: To mitigate the risk of unintentional disclosure of confidential information by employees, H.R. will refer newly onboarded employees to this policy and will require formal acknowledgement that it has been read, is understood, and will be applied.

Existing Employees: To mitigate the risk of staff falling victim to a cyber-attack, cyber security training, awareness communications and various testing/simulation methods will be used on an ongoing basis to both educate our staff and provide an assessment on how cyber aware the organization is.

E. Business Continuity

Data and system backups are a critical component of business continuity to ensure the County can quickly recover from not only cyber security incidents such as ransomware or malware attacks, but also from natural disasters, equipment failure or theft. Lacombe County performs encrypted backups on a nightly basis with a full copy of this encrypted backup moving to a secured offsite location on a weekly basis. The technology used in this backup process includes the ability to quickly restore data on an as-needed basis, which allows the I.T. Department to verify that the backup and restore mechanisms operate as expected.

F. Disaster Recovery Plan

The main objective of implementing a Disaster Recovery Plan (DRP) is to develop, test and document a well-structured and easily understood plan that will help the County recover as quickly and effectively as possible from a cyber attack or unforeseen disaster that interrupts County systems and business operations. To support the County's cyber security

operations, the I.T. Department will be responsible for developing a comprehensive, well-documented recovery plan that will facilitate an effective response to any cyber-related incident the County may face. The main components of the plan will include:

- Risk assessment of potential threats
- Inventory of I.T. assets
- Classification and prioritization of I.T. assets
- Defining recovery time objectives (RTO) and recovery point objectives (RPO)
- Disaster recovery setup
- Budget
- Testing and review principles

User's Acknowledgement:

I acknowledge that I have read, understand and agree to comply with this Cyber Security Policy as set forth above. I understand that failure to comply with this policy may result in disciplinary action, including termination, as well as legal action against me to seek damages, indemnification and costs.

Name _____ Signature _____

Date _____

References:
Lacombe County Policy AD(23) – Internet and Email Use
Lacombe County Policy AD(42) – Social Media Policy – Council
Lacombe County Policy AD(43) – Social Media Policy – Staff
Lacombe County Directive CS(5) – Computer Security and User Passwords

Approved:
Revised: