	Information Technology Data Breach Policy		
	Control Number	**Policy Date**	**Revision Date**
	HR058	10/06/25	New

Purpose

To establish the requirements for the breach response process, defining to whom it applies and under what circumstances, and including the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanism, privacy and security protection

Scope

All full time and budgeted thirty-two (32) hour employees and all regularly scheduled part time and seasonal/temporary employees. This policy also applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information, CJIS or Protected Health Information (PHI) of Scotland County members.

General Statement

Scotland County's Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Scotland County's established culture of openness, trust and integrity should respond to such activity. Scotland County Information Security is committed to protecting Scotland County's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. The policy shall be well publicized and made easily available to all personnel whose duties involve data

Policy Requirement

This policy mandates that any individual who suspects that a theft, breach or exposure of Scotland County's Protected data or Scotland County's Sensitive data has occurred must immediately provide a description of what occurred via e-mail to service@vc3.com, by calling 1-800-422-5941. This team will investigate all reported data breaches and exposures to confirm if a breach or exposure has occurred. If a breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place and work collectively with VC3 in determining the depth of the incident.

Once reported to VC 3, Scotland County Required Reporting Policy also requires reporting to the County Manager immediately.

Policy Confirmed theft, data breach or exposure of Scotland County Protected data or Scotland County Sensitive data:

As soon as a theft, data breach or exposure containing Scotland County protected data or Scotland County sensitive data is identified, the process of removing all access to that resource will begin.

The County Manager will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure;
- IT Applications;
- Risk Management;
- Finance (if applicable);
- Legal;
- Communications;
- Member Services (if Member data is affected);
- Human Resources;
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed;
- Additional departments based on the data type involved
- Additional individuals as deemed necessary by the County Manager.

In the case of confirmed theft, breach or exposure of Scotland County data the County Manager will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by Scotland County cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Develop a communication plan

The incident response team will work with Scotland County Manger, Public Information Officer, legal, and human resource department to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Ownership and Responsibilities

Roles & Responsibilities:

- Sponsors - Sponsors are those members of the Scotland County community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any Scotland County Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is designated by the County Manager, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

- Users include virtually all members of the Scotland County community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by the County Manager and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Human Resources.

Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text.

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) - Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) - Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data - See PII and PHI

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

Any questions or further guidance for policy interpretation and implementation should be directed to the County Manager.

Disciplinary

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination. Any third party partner company found in violation may have their network connection terminated. The county also reserves the right to pursue other remedies.

Rerefence

n/a (new as of 10/6/25)