County of Bedford, Virginia **Incident Response Policy**	
Information Technology Department	**Issue/Effective Date: May 9, 2023** **Approval Date: April 24, 2023** **Approved By: County Administration**

I. Overview and Policy Purpose

It is the employee's responsibility to report any and all information technology security incidents to IT. The purpose of this policy is to ensure prompt and effective detection, containment, and recovery from security incidents.

II. Scope

This policy applies to current and future Bedford County, VA and their employees. In addition, some third parties such as contractors or vendors may be required to abide by parts of this Policy if required by contract.

III. Guidelines

An information technology security incident is an indication of attempted or successful unauthorized entry to a system, an information attack on a system or network, or a disclosure of sensitive information contained in an information system. Information technology security incidents include:

- Attempted entry (failed or successful) to gain unauthorized access to a system or data; e.g., unauthorized scans and probes.
- Unexplained disruption or denial of service.
- Unauthorized use of a system for the processing or storage of data.
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent (e.g., malicious logic such as virus, worm or a Trojan horse).
- Poor security practices, such as exposure of passwords, etc.
- A disclosure of sensitive information contained in a system.

All Bedford County, VA employees will report any security incident that they become aware of or suspect to IT Director or designee.

A security incident is any breach of security policy, or any activity that could potentially put sensitive information, especially cardholder data, at risk of unauthorized access, exportation, use, disclosure, or modification.

Non-critical incidents generally have the following characteristics:

- *It is determined that there was no malicious intent (or the attack was not directed specifically at Bedford County, VA; or*
- *It is determined that no sensitive information (especially cardholder data) was accessed, exported, used, disclosed, or damaged in an unauthorized manner.*

Critical incidents generally have the following characteristics:

- *It is determined that there was malicious intent and/or an attack was directed specifically at Bedford County, VA; or*
- *It is determined that sensitive information especially cardholder data or personally identifiable information, may have been accessed, exported, used, disclosed, compromised, or damaged in an unauthorized manner.*

IV. Responsibilities

A. Employees

All individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents;
- Reporting any suspected security incident to the IT Director or designee;
- Assisting the IT Director or designee with ending the security compromise and mitigating its harmful effects, if possible.

B. Information Technology Department

The IT Director or designee is responsible for:

- Maintaining this policy;
- Characterizing all reported security incidents as “critical” or “non-critical”;

The IT Director or designee may consider their professional expertise and experiences when making these characterizations in accordance with laws, regulations, and PCI standards; maintaining procedures for responding to security incidents; and documenting all reported security incidents and their outcome.

The IT Director or designee and other members of management are jointly responsible for:

- Mitigating, to the extent possible, any harmful effects of security incidents;
- Deciding when it is appropriate to contact law enforcement officials about a security incident;
- The IT Director or designee is responsible for immediate notification to County Administration, legal counsel, and the carrier about any security incident compromises before any external parties or incident response service providers are engaged.

V. Legal Analysis for Reporting and Notifications

Bedford County, VA processes and maintains a vast amount of public, private, sensitive, and other internal use information that requires to be protected by Federal, Commonwealth, and other laws and

regulations. Examples include protected health information regulated by HIPAA, personally identifiable information such as financial account numbers or social security numbers, driver's license numbers, and credit card numbers. While not all-inclusive, below are references to various regulations that may require breach notification.

HIPAA Breach Notification Rule https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Virginia Data Breach Notification Requirements in accordance to §§2.2-603, 2.2-2009, and 2.2-5514 of the Code of Virginia, https://law.lis.virginia.gov/vacode/title18.2/chapter6/section18.2-186.6/

Payment Card Industry – Security Standards Council https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

VACORP Cybersecurity Event Reporting per Cyber insurance guidelines

VI. Compliance

This policy is relevant to the PCI DSS v3.2 Requirements 12.1, 12.4, 12.5, 12.10 and Virginia Locality Election Security Standards Requirement 2 Incident Response, Incident Reporting, 1.1.

Robert Hiss
County Administrator