Examples of Reportable Information Privacy and Security Incidents (not comprehensive)

1. Unauthorized Disclosure

   - Confidential or proprietary information is disclosed without authorization.

2. System Incapacitation

   - A system’s ability to function is impaired by a high volume of activity from various sources.
   - A resource such as power, network access, or routing tables is modified, degrading the system’s ability to perform normal functions.
   - A malicious code (virus, trojan horse, etc.) interferes with a system’s operation.
   - An asset is stolen, damaged, or destroyed.

3. System Tampering

   - A UserID is employed to gain access to system administrative functions without prior authorization.
   - A system weakness allows access to system administrative functions by unauthorized Users.
   - A valid UserID is permitted to gain access to system administrative functions without authorization.
   - Non-administrative personnel are allowed to perform administrative system functions.

4. Information Tampering

   - A UserID is employed to gain access without authorization to password files, protected or restricted data, licensed applications, software, or restricted applications, software, and/or code.
   - A system weakness allows unauthorized access to password files, protected or restricted data, licensed applications, software, or restricted applications, software, and/or code.
   - A theft of information assets provides access to password files, protected or restricted data, licensed applications, software, or restricted applications, software, or code.

5. Misuse of Information Technology

   - A User installs unlicensed software.

   - A User's account is employed in violation of legal statutes, regulations, or organization policies.

6. Unauthorized Access

   - A valid UserID is employed without authorization.

   - A system weakness is exploited, but no access is gained outside the account's authorizations.

   - A User's privilege to access information is higher than that which was authorized.

   - Access to facilities (buildings, rooms, secure areas) is gained without authorization.

   - A User's laptop or desktop computer is stolen.

7. Unauthorized Use

   - Any use of confidential or proprietary information for a purpose not specifically permitted based on the User's need to know.

8. Attempted Exploration of Information Assets

   - Illegal data gathering is directed against a system (port scanning, sniffing, net scanning, etc.).

   - Actions are attempted that could impair a system's ability to function.

   - Actions are attempted that could result in a system or information compromise.

9. Non-System Incidents

   - Physical Facility Access Incidents – Unauthorized access to facilities results in information asset exposure or compromise.

   - Physical Access to Information – Unauthorized parties gain access to confidential or proprietary information.

   - Equipment Control Incidents – Tenet information assets are exposed or compromised due to a lack of control over computing equipment.

- Media Control Incidents – Tenet information assets are exposed or compromised due to a lack of control over computing media.

- Physical Safeguards/Environmental Hazards – Tenet information assets are exposed or compromised due to an environmental hazard such as a tornado or thunderstorm.