Security Incident Reporting Guide

What is a Security Incident?

refers to an event or occurrence that affects or tends to affect data protection, or may compromise the availability, integrity, and confidentiality of personal data. It shall include incidents that would result to a personal data breach, if not for safeguards that have been put in place. A data breach is a type of security incident.

What is a Data Breach?

refers to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

availability breach - loss, accidental or unlawful destruction of personal data;

integrity breach - alteration of personal data;

confidentiality breach - unauthorized disclosure of or access to personal data.

What is a Personal Information?

any information that (a) can be used to identify the data subject to whom such information relates, or (b) is or might be directly or indirectly linked to a data subject

What is Sensitive Personal Information

1. refer to an individual's: race, ethnic origin, marital status, age, color, affiliations (religious, philosophical, or political), health, education, genetic or sexual life;

2. refer to any proceeding for any offense allegedly or actually committed by an individual, including the disposal of or the court's sentence in such proceeding;

3. are issued by government agencies peculiar to an individual (e.g., social security number, previous or current health records, licenses [including its denials, suspension, or revocation], tax returns, etc.);

4. are classified, as established by an Executive Order or a law enacted by Congress.

Types of Security Incident

1. Theft - Incident or events that resulted in the illegal transfer or storage of any personal data to unauthorized actors
    a. Physical Theft: This involves the physical stealing of devices such as laptops, smartphones, or external hard drives that contain sensitive data.
    b. Data Theft: Unauthorized access and extraction of data from systems, often through hacking or insider threats.
    c. Insider Threats: Employees or contractors with access to sensitive data who misuse their access for personal gain or malicious intent.
2. Malicious Code - Incident or events that resulted to a malicious code causing damage to personal data processing system

    a. Viruses: Malicious programs that attach themselves to legitimate files and spread across systems, causing damage or data loss.
    b. Ransomware: Malware that encrypts data and demands a ransom for its release.
    c. Trojans: Malicious software disguised as legitimate applications, which can steal data or create backdoors for further attacks.
3. Hardware Failure - Incidents or events that resulted to the termination of the ability of all or part of the physical components of a personal processing system to perform a required function
    a. Disk Failures: Physical damage or wear and tear of storage devices leading to data loss.
    b. Server Failures: Malfunctions in server hardware that can cause data unavailability or loss.
    c. Power Failures: Sudden loss of power can cause data corruption or loss, especially if there are no backup systems in place.
    d. Component Failures: Failures in critical components like motherboards or power supplies that can lead to system crashes and data loss.
4. Operations Error - Incidents or events that resulted due to improper execution of the organizations operational procedures
    a. Network Misconfigurations: Incorrectly setting up network devices, such as firewalls or routers, which can expose sensitive data to unauthorized access.
    b. Software Misconfigurations: Improper settings in software applications that can lead to vulnerabilities and potential breaches.
    c. Accidental Data Deletion: Unintentional deletion of important files or databases by employees.
    d. Incorrect Data Handling: Mishandling of sensitive data, such as sending confidential information to the wrong recipient.
    e. Incomplete Backups: Failing to back up all necessary data, leading to data loss in case of a system failure.
    f. Corrupted Backups: Backups that are corrupted and unusable when needed for data recovery.
    g. Excessive Privileges: Granting users more access rights than necessary, increasing the risk of data misuse.
    h. Failure to Revoke Access: Not revoking access rights from employees who no longer need them, such as former employees.
5. Identity Fraud - Incidents or events that resulted to a successful attempt of using someone's identity
    a. Phishing: Deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity in electronic communications.
    b. Credential Theft: Stealing login credentials through various means, such as keylogging or phishing, to gain unauthorized access to systems.
6. Hacking - Incidents or events that resulted to intentionally accessing a computer system or personal data processing system without the authorization of the user or the owner
    a. Unauthorized Access: Gaining access to systems or data without permission, often through exploiting vulnerabilities.
    b. Data Breaches: Stealing sensitive information.
7. Software Failure - Incidents or events that resulted to the termination of the ability of all or part of the programs, procedures, rules, and associated documentation of a personal data processing system to perform a required function
    a. Bugs and Glitches: Software errors that can lead to data corruption or loss.
    b. Unpatched Vulnerabilities: Failing to update software, leaving systems exposed to attacks.
    c. Compatibility Issues: Software that doesn't work well with other systems, causing failures.
8. Design Error - Incident or events that resulted to incorrect, incomplete, or poorly communicated design of a system or software to reduce the possibility of user making mistakes
    a. Flawed Security Architecture: Poorly designed systems that are inherently insecure.
    b. Misconfigured Systems: Incorrect settings that leave systems vulnerable to attacks.

    c. Insecure APIs: Poorly designed application programming interfaces that expose data.
    d. Weak Encryption: Using outdated or weak encryption methods that can be easily broken.
9. Sabotage/Physical Damage - Incidents or events that resulted to an internal or external deliberate act of destruction or disruption of the organization's personal data processing activities
    a. Insider Threats: Employees intentionally damaging or stealing data.
    b. External Attacks: Deliberate actions by outsiders to disrupt operations or steal data.
    c. Denial of Service (DoS): Overloading a system to make it unavailable to users.
    d. Natural Disasters: Events like floods or earthquakes that damage hardware.
    e. Theft or Vandalism: Physical theft or destruction of equipment.
    f. Power Surges: Electrical spikes that damage hardware.
    g. Fire: Incidents that destroy physical infrastructure and data storage devices.
10. Misuse of Resources - Incidents or events that resulted to the deviation from the intended use of any element of a personal data processing system needed to perform required operations
    a. Unauthorized Use: Using company resources for personal gain or unauthorized activities.
    b. Unapproved Software Installation: Installing unauthorized software can lead to security vulnerabilities and misuse of system resources.
11. Communication Failure - Incidents or events that resulted to unexpected release of personal data through any communication means or platforms
    a. Network Outages: Interruptions in communication networks that disrupt data flow.
    b. Miscommunication: Incorrect or incomplete information sharing that leads to security lapses.
    c. DNS Failures: Issues with the Domain Name System that disrupt internet services.
    d. Email Server Outages: Failures in email servers that prevent communication.
12. User Error - Incidents or events that resulted to mistake of human action or inaction that produced an unintended result
    a. Accidental Deletion: Unintentionally deleting important data.
    b. Improper Handling: Mishandling sensitive information, such as sending it to the wrong recipient.
    c. Weak Passwords: Using easily guessable passwords that compromise security.
    d. Improper Disposal: Failing to properly dispose of sensitive documents or devices.
13. Third Party/Service Provider - Incidents or events that exposed personal data of the organization caused by their official third party partners or service providers
    a. Vendor Breaches: Security incidents originating from third-party vendors.
    b. Supply Chain Attacks: Compromising a supplier to gain access to a target organization.
    c. Cloud Service Breaches: Incidents where cloud service providers are compromised.
    d. Third-Party Software Vulnerabilities: Security flaws in software provided by third parties.
14. Others - Incidents or events that do not fall to the criteria mentioned above

Security Incident Response Team

The SIRT will be responsible for the following:

1. Investigate and assess suspected security incidents in coordination with all concerned units and offices of the University.
2. Recommend remedial measures to be performed by the Process Owner and other concerned units or offices of the University in relation to a suspected security incident.
3. Accomplish an Incident Report.

The following offices and individuals shall perform their respective functions and responsibilities:

DPO

1. Main point of contact for all reports of a suspected security incident.
2. Notify the NPC and/or affected data subjects when required by DPA.

3. Assist the University President, the SIRT, and Process Owners in the performance of their functions under this Policy.

University President

1. Approve, reject, or otherwise take action on the findings or recommendations of the SIRT.
2. Appoint the members of the SIRT.
3. Approve, reject, or otherwise comment on proposed revisions to this Policy.

Departments/Process Owners

1. Submit an Incident Report to the DPO when a reported incident involves its data processing system or any personal data under its control, including those being processed by a service provider or an authorized third party.
2. Implement security measures that aim to:
    a. avoid or minimize security incidents
    b. stop an ongoing security incident
    c. contain, limit, or mitigate the impact of a security incident
3. Cooperate with and extend assistance to the DPO and the SIRT in resolving each reported incident.

Security Incident Reporting Procedure

1. An incident must involve a data processing system of the University or personal data under its control or custody. This includes data being processed by service providers or any other authorized third parties.
2. Any LCUP personnel who becomes aware of or suspects an incident as described in the previous section must promptly notify the DPO using the Data Security Incident Form. If a notification is sent to or received by another University office, it should be immediately referred to the DPO to ensure timely action.
3. To notify the DPO of an incident, individuals should submit a Data Security Incident Form as prescribed by the DPO. If the Data Security Incident Form is unavailable, the notifying party must provide the following information:
    a. Name
    b. Email Address or contact number
    c. Details of Incident
        I. Type of Security incident
        II. Date and Time of Security incident
        III. Number of persons affected
        IV. Name of department/unit processing the information

Incident Response Procedure

1. Incident Reporting: Upon discovering a security incident, it must be reported to the Data Protection Officer (DPO) within 24 hours.
2. Initial Assessment: The Security Incident Response Team (SIRT) will conduct an initial assessment to determine the scope and impact of the incident.
3. Investigation: Within 48 hours of the initial assessment, the SIRT will perform a thorough investigation to identify the cause, affected systems, and data involved.
4. Reporting and Remedial Measures: Following the investigation, the SIRT will compile a report detailing the findings and recommend remedial measures to prevent future incidents.

5. Post-Incident Review: After implementing remedial measures, the SIRT will conduct a post-incident review to evaluate the effectiveness of the response and identify areas for improvement.

Data Breach Notification and Reporting to the National Privacy Commission

The National Privacy Commission and affected data subjects shall be notified by the University within seventy-two (72) hours upon knowledge of, or when there is reasonable belief by the University that, a personal data breach requiring notification has occurred.

Notification of personal data breach shall be required when sensitive personal information or any other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the University or the National Privacy Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.