AGUSAN DEL SUR STATE COLLEGE OF AGRICULTURE AND TECHNOLOGY
Bunawan, Agusan del Sur

Computer Emergency Response Team

CERT Manual

Notice: Information contained in this document is classified as Agusan del Sur State College of Agriculture and Technology (ASSCAT) Confidential Proprietary. No person outside ASSCAT shall have access to the information contained in this document unless the College approves it. Otherwise, it is the responsibility of the person knowing the information contained in this document to ensure its confidentiality of it and to prevent unauthorized access to it.

Uncontrolled copy if printed/photocopied (unless specified otherwise)

CONFIDENTIAL

1.1 Introduction

The information age has revolutionized information and communication processing, making access to data incredibly convenient for everyone. Cyberspace, including internal organizational networks, fosters virtual communities and serves as a superhighway for data convergence. However, its vastness exposes it to various threats, risks, and vulnerabilities.

The rise in computer security incidents, accidental or deliberate, can affect individuals and organizations alike, with potential impacts ranging from minimal to catastrophic. This underscores the critical importance of computer security for everyone.

Responding quickly and efficiently to any incident is crucial. It helps minimize costs associated with maintaining, recovering, and ensuring operational continuity. Recognizing this, the Computer Emergency Response Team (CERT) Manual was developed as part of the Agusan del Sur State College of Agriculture and Technology's Information Security Management System.

The manual establishes general policies and outlines processes, procedures, and protocols for handling security incidents. It draws from relevant laws and regulations, ISO/IEC International Standards on Information Technology, international frameworks from other CERT bodies, documented best practices, and publicly available online documents on security standards.

1.1.2 Brief Overview of the Manual

This manual is divided into several chapters and sections to facilitate easy access to information. Topics and subjects are clustered together to facilitate easy updates and revisions without rewriting the entire manual.

1.1.3 Applicability

This manual applies to all personnel assigned to the computer emergency response team, including internal and external groups and individuals employed by the institution.

1.2 References

ISO/IEC 27000	Information technology — Security techniques — Information Security Management Systems — Overview and Vocabulary
ISO/IEC 27002	Information technology — Security techniques — Code of practice for information security controls
ISO/IEC 24762	Information technology – Security techniques – Guidelines for information and communications technology disaster recovery services
ISO/IEC TR 18044	Information technology – Security techniques – Information security incident management
NIST SP 800-61 Rev.2	National Institute of Standards and Technology – Computer Incident Handling Guide
NIST SP 800-30 Rev.1	National Institute of Standards and Technology – Information Security
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems

*NOTE: *The latest version of the above references is to be deemed applicable.*

1.3 Terms and Definitions

Purpose

The purpose of this section is to define terms related to R.A. 10173 and the Information Security Management System (ISMS) ensuring that all users a common and basic understanding and interpretation of the terms throughout this manual.

Scope

The terms and definitions provided in this manual encompass commonly used terms within the ISMS.

Attack
Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organization.

Asset
Any item that has value to the organization

Attribute
Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

Authentication
Provision of assurance that a claimed characteristic of an entity is correct

Authenticity
Property that an entity is what it claims to be

Availability
Property of being accessible and usable upon demand by an authorized entity

Business Continuity
Procedures and/or processes for ensuring continued business operations

CERT

Computer Emergency Response Team (CERT) or Computer Security and Incident Response Team (CSIRT) refers to

“An organization that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security”. At present, “both terms (CERT and CSIRT) are used synonymously” (ENISA, 2015 and ENISA, 2015a).

Computer security also known as cyber security or IT security
Is the protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide

Confidentiality
Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Consequence
The outcome of an event affecting objectives.

Control
Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature.

Control Objective
Statement describing what is to be achieved as a result of implementing controls.

Corrective Action
Action to eliminate the cause of a detected non-conformity or other undesirable situation.

Data
Collection of values assigned to base measures, derived measures and/or indicators. This definition applies only within the context of ISO/IEC 27004:2009.

Electronic Discovery (e-Discovery)
is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing Electronically
Stored Information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries.

Effect
Is a deviation from the expected — positive and/or negative.

Effectiveness
The extent to which planned activities are realized and planned results achieved.

Efficiency
Relationship between the results achieved and the resources used.

Event
Occurrence or change of a particular set of circumstances

Guideline
Description that clarifies what should be done and how to achieve the objectives set out in policies.

ICT systems
Hardware, software, firmware of computers, telecommunications and network equipment or other electronic information handling systems and associated equipment.

Information security
Preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information security event
It refers to an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

Information security incident
It is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

Information system
Application, service, information technology asset, or any other information handling component.

Infrastructure
Facilities and equipment to enable the ICT DR services, including but not limited to power supply, telecommunications connections and environmental controls

Integrity
Property of protecting the accuracy and completeness of assets

Management
Coordinated activities to direct and control an organization

Management system
Framework of guidelines, policies, procedures, processes and associated resources aimed at ensuring an organization meets its objectives

Measure
Variable to which a value is assigned as the result of measurement

Measurement
Process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria

Object
Item characterized through the measurement of its attributes

Organizations
Entities which utilize ICT DR services

Owner
Identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. This term does not mean that the person has any property rights to the asset.

Policy
Overall intention and direction as formally expressed by management

Procedure
Specified way to carry out an activity or a process

Process
Set of interrelated or interacting activities which transform inputs into outputs

Record
Document stating results achieved or providing evidence of activities performed

Reliability
Property of consistent intended behaviour and results

Review
Activity undertaken to determine the suitability, adequacy and effectiveness (2.22) of the subject matter to achieve established objectives

Review object
Specific items being reviewed

Risk
Combination of the probability of an event and its consequence

Risk acceptance
The decision to accept a risk

Risk analysis
Process to comprehend the nature of risk and to determine the level of risk

Risk assessment
The overall process of risk identification, risk analysis and risk evaluation

Risk management
Coordinated activities to direct and control an organization about risk.

Stakeholder

A person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

Third-party
A person or body that is recognized as being independent of the parties involved, as concerns the issue in question

Threat
Potential cause of an unwanted incident, which may result in harm to a system or organization

Validation
Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

Verification
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled.

Vulnerability
Weakness of an asset or control that can be exploited by one or more threats

1.4 Acronyms and Abbreviation

BIA Business Impact Analysis

CERT Computer Emergency Response Team

DDoS Distributed Denial of Service

FW Firewall

ICT DR Information and Communications Technology Disaster Recovery

IDS Intrusion Detection System

IEC International Electrotechnical Commission

ISMS Information Security Management System

CERT National Computer Emergency Response Team

NCSP National Cybersecurity Plan

SMTP Simple Mail Transfer Protocol

ISO International Standards Organization

MDF Main Distribution Frame

PDA Personal Digital Assistant

POC Point of Contact

SIEM Security Information and Event Management

UPS Uninterrupted Power Supply

Chapter 2.0 Computer Emergency Response Team Structure

Introduction

This section shall provide the organizational structure (See Annex A) to guide the institution in the planning, formulation, development, implementation, management and review of the Computer Emergency Response Team (CERT). It will describe the key roles and responsibilities of assigned owners and provide a clear scope of accountabilities of individuals, team members and groups (internal and external) that will be involved in the development of the guidelines for the implementation of the computer emergency response team management plan, treatment and structured approach for responding to the information security incident, and the creation of the CERT.

The factors critical to the successful implementation of the computer emergency response plan are, but not limited to the statement indicated within this document, the following:

1. An established information security policy, objectives and activities to respond with adequacy and readiness when an incident or event occurs.

2. An established approach and framework of implementing, maintaining, monitoring and improving computer emergency response plan that is consistent with the institutional requirement and culture.

3. A good understanding of the information security requirements, risk assessment and risk management to respond with an appropriate course of action that will direct the CERT on implementing and managing the computer emergency response plan.

4. Continuous monitoring and evaluation of the performance in the implementation of the ISMS for improvement.

Chapter 2 Roles and Responsibilities

Scope

This section covers the roles and responsibilities of members assigned ownership of tasks specific to the guidelines developed for managing computer emergency response plans.

2.1 Information Security Committee

The Information Security Committee ensures cybersecurity policies, plans and standards are formulated, implemented, monitored, and evaluated. It also monitors and evaluates the outputs, outcomes, and strategic impacts of all cybersecurity programs and projects, including the CERT, and provides strategic recommendations.

Functions related to the CERT include:

a. Reviewing and evaluating the performance of the CERT;

b. Reviewing and evaluating the results of CERT operations;

c. Reviewing and evaluating the results from the analysis conducted on the data collected, gathered and added into the database for incidents/events and the corresponding immediate responses made by the CERT;

d. Evaluating the policies, procedures and processes to determine their applicability and effectiveness in addressing and responding to an incident or event by:

- Guiding the appropriate changes based on the results from review activities and the services offered by the CERT (Refer to Guidelines for CERT Services).
- Providing a framework for continuous improvement of the CERT.
- Recommending appropriate plans to ensure CERT elements comply with relevant local/international IT standards and mandatory laws/regulations.

e. Develop a well-structured process for detecting, reporting, assessing and managing information security events and enabling tools, methodologies and practices for:

- Rapid identification and response to security events or incidents;
- Enhancing overall security through consistent implementation of solutions; and
- Providing means of preventing future similar information security incidents.

f. Develop a well-structured approach to incident response that will create a better focus on incident prevention.

g. Develop a well-structured approach to the incident response that will provide guidance and direction for prioritizing appropriate courses of action when conducting computer emergency investigations.

h. Provide input to Computer Emergency Response policies review by:

- Providing data collected from reported security incidents and immediate responses by the CERT;
- Updating and strengthening of capability and capacity to collect and gather information on information security incidents and events; and
- Consolidating data for availability and ease of access of the members of the CERT.

2.2 Computer Emergency Response Team

The CERT is responsible for receiving, reviewing, and responding to computer security incident reports and activities. It ensures systematic information gathering, dissemination, coordination, and collaboration among stakeholders, particularly other Computer Emergency Response teams, to mitigate information security threats and cybersecurity risks.

Primary functions include:

- Collecting and gathering data upon initial detection or reporting of events/incidents.
- Creating initial information classification approving decisions regarding controls and access privileges
- Perform periodic reclassification
- Regularly reviewing and updating management of risk changes.

2.2.1 Roles and Responsibilities

Role	Function	Duties and Responsibilities
Point of Contact (POC)	Provides frontline service in the implementation of the Computer Emergency Response which establishes the first POC with users or reporters of any detected incident or event	1. Receiving calls and acting as the switchboard operator; 2. Screening and filtering data for information classification; 3. Communicating relevant calls to the CERT CISO; and 4. Providing administrative support to the operation of the team.
Analysts	Perform analysis and evaluation of information to determine its relevance prompting immediate response and initiating actions to respond to the incident or event.	1. Initial collection and data gathering of information on detected and reported incidents or events; 2. Creating initial information classification; 3. Opening and assigning incident report ticket number upon classifying information as relevant; 4. Closing of incident report ticket number when information is classified as false positive; 5. Communicating results to personnel or group of personnel with specific tasks to respond to the incident or event; 6. Perform appropriate responses with the immediate objective of de-escalating the

Role	Function	Duties and Responsibilities
		level of vulnerability and adverse impact to the organization; 7. Logging of responses and actions taken to update the database; and 8. File incident reports on assigned cases.
Chief Information Security Officer (CISO) / Team Leader	perform supervision and evaluate reported incidents before assigning caseloads to Analysts with appropriate set skills in performing analysis and evaluation of the data gathered and collected during the initial reporting stage.	1. Assign caseloads to CERT Analyst; 2. Ensure regular review for value and updates to manage changes to risk; 3. Monitor close/open incident report tickets, resolved/unresolved incidents or events; 4. Ensure that appropriate responses are immediately implemented and communicated to personnel tasked to perform specific roles; 5. Ensure that frontline personnel and analysts log and update records immediately and accordingly; 6. Decides to escalate or de-escalate incidents per assessment; 7. Evaluate the performance of Analysts and POCs; 8. Prepare a summary of incident reports. 9. Submit analysis results of incidents classified as false positive for input during review to determine the capability of frontline personnel to collect and gather substantial information; 10. Regular review of collected and gathered data to evaluate information value; 11. Prepare reportorial requirements for operational, administrative, and budgetary purposes.
Supervisor	Supervise the CERT team and external groups assigned to perform support services in responding to information security incidents or events.	1. Interface and report to the College President a summary of incident response activities and series of actions taken by CERT; 2. Submit a summary of resolved and unresolved cases for input during the review and improvement of the information security incident response plan;

Role	Function	Duties and Responsibilities
Systems Compliance and Management Auditor	In charge of information security and IT system compliance including evaluation of the implementation in processes and procedures.	1. Evaluate whether the internal controls are designed and operating as contemplated in the assessment control risk; 2. Validate and confirm the assessment of control risks based on substantive procedures and other audit evidence obtained during the conduct of the audit; 3. Discuss with the Management and agree on the Audit Plan, Audit Methodologies, Resources, Timeframe and reporting requirements for the assignment; and 4. Make Management aware as soon as practical and at an appropriate level of responsibility of material weaknesses in the design or operation of the internal control systems that have come to the Auditor's attention.

Chapter 3.0 General Policies

Introduction

Computer and information security is paramount for government, private entities, and individuals alike. In today's digital age, organizations and individuals heavily rely on information technology and systems to fulfill their missions and operations.

However, these systems are susceptible to various threats, including incidents and events that can compromise the confidentiality, integrity, and availability of information. Such threats, arising from both known and unknown vulnerabilities, can cause significant harm to organizational operations, assets, individuals, other organizations, and even the Philippine government.

To safeguard against these risks, it is imperative to detect and report threats early on. All levels of an organization must understand their roles and responsibilities in maintaining information security.

Compliance with Philippine laws, such as the Data Privacy Act of 2012 and the Cybercrime Prevention Act of 2012, is essential. These laws establish the legal framework for protecting personal data and addressing cybercrimes. By adhering to these regulations, organizations demonstrate their commitment to safeguarding sensitive information and ensuring the security of their systems.

A robust information security program not only protects organizational assets but also fosters public trust and confidence.

Scope

1. The scope of this section includes the protection of the confidentiality, integrity, and availability of information.
2. The framework for managing information security policy and reporting of information security incidents applies to all students, employees, and other involved persons, as well as all systems throughout the institution.

3.1 General Policy on CERT Documentation

a. It is the policy of the institution that information in all its forms, whether written, spoken, recorded electronically, or printed, shall be protected from accidental or intentional unauthorized modification, destruction, or disclosure throughout its lifecycle.

b. All policies and procedures shall be documented and made available to individuals responsible for their implementation and compliance to RA 10173.

c. All documentation, including electronic forms, shall be retained for at least six (6) years after its last revision. If any specific policies on records archiving and disposition provide a retention period different from that established by the institution's records disposition schedule, the retention period established by law or regulation shall govern.

d. All documentation shall be periodically reviewed at regular intervals to ensure its continued appropriateness and applicability over time.

3.2 Policy on CERT Accountability

- It is the policy of the institution to ensure the integrity and reliability of the institutional digital presence as part of its commitment to good governance. The institution shall provide a cost-efficient service and set of standards, which will serve as a means for actors both within and outside of government to enforce accountability.

- Establish control in reporting all computer emergency incidents and events through appropriate channels with the creation of the CERT.

Chapter 4.0 Protocols and Classifications

Introduction

The institution has established protocols to activate the CERT (Computer Emergency Response Team) once an incident report is received. This section also contains ~~a~~ classification of reports that will be used as a reference when assessing incidents and planning appropriate activities and responses.

4.1 Activation of CERT Protocol

Scope

This section covers the CERT Protocol of the institution in responding to incident reports.

a. Activate CERT protocol within 24 hours after confirming the validity of the incident.

b. Ensure proper coordination between relevant CERT personnel to keep them informed of the current status of the information security incident.

c. Notification chart shall be observed and followed accordingly.

4.2 Assessment Protocol

a. The CERT Analyst shall determine the category and severity of the incident and coordinate with the CERT Team Leader;

b. The CERT Team Leader shall discuss and determine the next course of action;

c. Upon assembling the CERT Team, an assessment is executed and reviewed to ensure all pertinent facts are established;

d. All discussions, decisions and activities must be documented; and

e. Designated persons will take action to notify appropriate internal and external groups, as necessary:

1. Internal Communication

   - On-duty team members shall notify all team members.
   - The CERT Team Leader shall notify all concerned and provide ongoing
   - The CERT Team Leader shall issue and direct all sensitive internal communications;
   - The Point of Contact (POC) will issue all public internal communication.

2. External Communication

   - All external communication and notification shall be approved by the College President.
   - The institution shall establish communication with the relevant third party, as appropriate for the circumstance.
   - The institution shall notify appropriate agencies, including the NPC (National Privacy Commission).
   - CERT members shall assist in determining if other parties, such as ISPs, should be notified.
   - The institution shall determine if, how, and when the media should be notified, and respond to all media inquiries.

3. Report Originator Notification

   - The Report Originator is informed that the incident has been reported and recorded, and that the investigation is in progress.
   - The Report Originator is provided with feedback and updates on the status of the investigation at every completed stage of the incident response process, including information required to escalate or de-escalate the process.
   - The Report Originator is notified of the results, closure of the investigation, and recommendations.

4. Status

   - The CERT shall assume responsibility for preparing and issuing communications within 48 hours after completing stages in an incident response activity to CERT members, the Information Security Committee, top management and other interested parties.

- Communications may include meetings, video conferencing, teleconferencing, email, telephone, voice recordings, social media or other means deemed as appropriate.
- The frequency and timeliness of communications are established and revised throughout the lifecycle of the incident.

4.3 Containment Protocol

a. The CERT shall determine the cause and prompt the execution of appropriate activities and processes required to quickly contain and minimize the immediate impact on the institution, the Report Originator, and other relevant stakeholders (if applicable)

b. Containment activities designed for execution have the following objectives:

- Counteract the immediate threat.
- Prevent propagation or expansion of the incident to other systems within the organization.
- Minimize actual and potential damage.
- Restrict knowledge of the incident to authorized personnel only.
- Preserve information relevant to the incident.

4.4 Corrective Measures Protocol

a. The CERT shall determine and promptly execute appropriate activities and processes required to restore the system to an acceptable and secure operational state.

b. Corrective measures designed for execution have the following objectives:

1. Secure the processing environment.
2. Restore the processing environment to its acceptable and secure state.

4.5 Closure Protocol

a. The CERT shall be actively engaged throughout the lifecycle of the information security incident.

b. The CERT shall continuously assess the progress and status of all containment and corrective measures.

c. The CERT shall determine the point at which the incident is considered closed or resolved.

4.6 Post Incident Review Protocol

a. All information security incidents-related activities are reviewed at regular intervals;
b. All members of the primary and secondary CERT teams should participate:

- The CERT shall host the post-incident review after each incident has been resolved and should be scheduled within 2 to 3 weeks after the incident has been remediated.

- The CERT review shall examine the incident and all related activities to improve and refine the overall incident response process.

c. Recommendations, discussions, and assignments for changes to policies, processes, protocols, procedures, or guidelines are documented for distribution to the CERT members.

d. The CERT shall conduct follow-ups with the report originator, third parties or other relevant stakeholders, as required or appropriate.

Chapter 5.0 General Guidelines

Introduction

CERT shall offer and provide various services related to information security.

5.1 List of CERT Services

Scope

This section covers the type of services that the CERT will provide. It also serves as reference material for capacity and capability development, strengthening CERT’s ability to respond to any incident or event.

a. **Incident Response** – Respond to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats. It employs mitigation, preparedness, and response and recovery approaches, as needed, to maximize the survival of life, the preservation of property, and information security.

b. **Actionable Security Intelligence** – Refers to the real-time collection, normalization, and analysis of data generated by users, applications, and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insights that reduce risk and operational effort for organizations of any size.

c. **Early Warning System** – A cyber-attack warning system that can be a powerful tool for providing early warnings about related attacks, both physical and virtual. A common technique used by attackers is to deploy a denial-of-service attack as a distraction while a more sinister attack occurs.

d. **ICT Equipment Testing Lab** – A local test laboratory contributes to the development of the institution by providing inputs that enable project validation and improvement. In addition, it promotes the growth of knowledge and supports regulatory agencies in the certification process.

e. **Web Intelligence (WEBINT)** - Exploits Artificial Intelligence (AI) and advanced information technology on the Web and Internet. It is a crucial and urgent research field for business intelligence in IT. WEBINT efficiently identifies intelligence available in open source (OSINT). Structuring and visualizing web-based information allows analysts to uncover tactical information such as technical indicators, and strategic insights like the changing sentiment in troubled regions.

5.2 Guidelines on Orientation and Preparation of CERT Personnel

Introduction

This section establishes guidelines to prepare personnel assigned to manage and handle responses to information security incidents or events. It provides ample preparation for individuals with specific roles and directions for team members in implementing the CERT.

Scope

This section covers information and guidelines for preparing people, personnel, and teams assigned to respond to any incident or event and to implement the national computer emergency response team management plan.

Target Audience

This section is intended for personnel who are:

1. Assigned as the POC or tasked with receiving collecting and compiling reported cases of events during the initial contact (whether through human means or automated systems).

2. Responsible for managing, supervising and directing the members of the CERT.

   a. Orientation of personnel assigned as the initial POC shall include:

      - Familiarity with the forms used for first and second assessments.
      - Familiarity with the different classifications and taxonomy used for incident response.
      - Familiarity with the key processes of incident response.
      - Familiarity with the flowchart for handling incident response.
      - Familiarity with the protocols for communicating and endorsing collected and compiled information for second assessment to CERT members.

- Understanding the importance of proper logging and recording of the event, including accuracy in time-stamping, event source, reporter details, etc.
- Understanding the importance of updating and recording of events into the database system for information security including recording of data on "false alarms" for future reference.
- Recognizing that the time taken to log the report for the first assessment affects the CERT's ability to respond effectively.

b. Orientation for personnel assigned to the CERT and tasked with responding to incidents or events detected or reported after the initial POC shall include:

- Familiarity with the forms that are used for first and second assessment.
- Familiarity with the different classifications and taxonomy used for incident response.
- Familiarity with the key processes of CERT.
- Familiarity with the flowchart of handling incident response.
- Familiarity with the communication protocols after event evaluation and early impact assessment has been conducted and endorsed to the CERT for escalation for further assessment and/or decisions that are required.
- Understanding the importance of accurate and appropriate logging of records and data for later analysis.
- Understanding the importance of updating the information security event or incident database.

c. Orientation of personnel assigned with the responsibility of managing the CERT shall include:

- Implementing a regular monitoring system to track and monitor all reported incidents and events.
- Reviewing the procedures for evaluating the applicability of the CERT.
- Establishing Treatment and handling procedures for internal security breach protocols.
- Establishing training program requirements for continuous development and capability building for personnel.
- Developing communication plans with other stakeholders.
- Defining escalation processes and procedures.
- Activating procedures for crisis management.

5.3 Guidelines on Reporting and Submitting Incident Reports

Introduction

As discussed in previous sections, time is a crucial factor in determining the ability of the CERT to respond to any reported event. Providing initial information about an information security event and determining the information security incident will prompt the appropriate people to respond according to the situation and urgency of the response requirement.

Scope

This section provides general guidelines on reporting, completing, and submitting an information security event and incident.

a. If a person suspects an information security event is in progress or may have occurred especially if it may cause substantial loss or damage to the institution, the report should be completed and submitted immediately.

b. The information provided be used to initiate appropriate assessment which will determine whether the event is to be categorized as an information security incident or not and if remedial measures are necessary to prevent or limit any loss or damage;

c. If the person reviewing the already completed or partly completed form is assigned to analyze the reports, the event needs to be categorized as whether it is an information security incident or a false alarm;

d. If the person reviewing the information security event and incident forms is a member of the CERT, then the incident form should be updated as the investigation progresses and related updates made to the information security event/incident database;

e. As much as possible, the form should be completed and submitted electronically, including when it is thought possible that the system is under attack and reporting forms can be read by unauthorized people, then alternative means of reporting should be used:

   - Alternative means or forms of reporting include in person, by telephone, email, text messaging or social media;
   - Provide only factual information and avoid speculating to complete the fields within a specified period (Please refer to Phase 2 Procedure) where it is appropriate to provide information that cannot be confirmed, state the information that is unconfirmed and annotation information that may lead to what may be true;
   - Always provide full contact details when submitting the completed form. There may be a necessity to contact the person who filed the report either very soon or at a later date to obtain further information concerning the report;

- Information that was provided during the report discovered to be inaccurate, incomplete or misleading at a later date is amended and resubmitted to update the record and log the correct information into the database; and
- Closure of the report will update the database or if the event has not been fully resolved and tagged as open, the records are still updated.

5.4 Guidelines on Handling Incident Response

Introduction

This section establishes the guidelines for handling responses to information security incidents or events. It provides direction in determining whether information security events escalate to information security incidents. When an information security event is detected and reported (by human or automated means), it initiates a series of phases and stages prompting the CERT to respond accordingly.

Scope

This section covers only guidelines on handling reported incidents and events for Information Security.

Target Audience

This section is intended for personnel who are:

- Assigned as the POC or tasked with receiving, collecting, and compiling reported cases of events during the initial contact (whether by human means or automated).
- Responsible for managing, supervising, and directing the members of the CERT.

a. Detection Reporting

- Incident events detected and reported either by human or automated feed shall be immediately logged into the information security incident monitoring and tracking system.
- Reported incidents or detected events shall be communicated immediately to the CERT.
- Communicated reports shall be logged immediately to update records.
- Always update the system with changes or responses associated with the incident report ticket number.
- Ensure logging and monitoring systems comply with the Data Privacy Act regarding the collection and processing of personal data.

b. Assessment Decision

- Information gathered and collected shall be submitted to the CERT.
- False positive results from the initial assessment shall also be logged into the system to track all reported events and incidents in compliance with data protection laws.
- Team Leaders assigning caseloads to CERT Analysts shall log and record incident report ticket numbers to update the database.
- An initial assessment containing relevant information shall be assigned to a CERT Analyst for further analysis and evaluation.
- Results from the second assessment shall be recorded and logged into the system.
- Communicate results for immediate response to CERT members, the technical support team, and other external support groups.
- Terminate or close the incident report ticket number by updating the system when cases are concluded as resolved.

c. Response

1. A list of personnel tasked and assigned with specific roles in CERT shall be regularly updated and posted to message boards;

2. Immediate objectives for responding to incidents or events are to lower the level of vulnerability and impact;

    - Adverse impact, risk levels, and associated threats and vulnerabilities shall be immediately evaluated and assessed to initiate various controls and appropriate levels of responses.
    - Immediate response shall be documented accordingly.
    - Reports shall be completed and filed immediately to update the system.
    - First responders to the reported incident or event in breach of information security shall conduct appropriate turnover procedures.
    - Log appropriate tagging of incident reports, e.g. closed/open, resolved/unresolved.
    - Immediate responses to reported events and detected incidents shall be evaluated regularly to determine the effectiveness of these responses and improve the system of responding to any information security breach.

5.5 Guidelines on Collecting and Gathering Data

Introduction

This section establishes the guidelines for collecting and gathering data and information for analysis that will direct the CERT to respond accordingly.

Scope

This section will cover only guidelines on collecting and gathering data for initial and second assessments on reported and detected incidents and events.

Target Audience

This section is intended for personnel who are:

1. Assigned as the POC or tasked with receiving, collecting and compiling reported cases of events during the initial contact (whether by human means or automated).

2. Responsible for managing, supervising and directing the members of the CERT

a. Guidelines on Collecting and Gathering Data and Information for Analysis

- Events or incidents that are detected and reported either by human or automated means shall be logged immediately and recorded appropriately into the system.
- Information, after it has been collected, shall be classified according to information categories.
- Reported incidents or events shall be classified according to their potential impact on the organization: limited adverse effect, serious adverse effect, or severe/catastrophic adverse effect.
- This information shall be classified and rated based on its security objectives: Confidentiality, Integrity, and Availability of Information.
- Data or information shall also be evaluated according to the sources of threats which can occur on three levels: the organizational level, the mission or business process level, and the information level;
- Information that has been collected shall be classified according to its type. This can be adversarial, accidental, structural or environmental;
- Once data or information is collected, it shall also be tagged according to its characteristics and the range of its effect;

    - Information collection and data gathering shall be complete and substantial to provide analysts ample data to perform analysis which will initiate immediate response or prompt a series of incident response activities;

- Time stamping and recording of events are crucial. It is therefore very important for the person collecting data to determine the time the event or incident occurred or was initially detected and reported. Time stamping and recording of events should be precise and comply with legal standards.
- Information that is classified as "false" positive shall be logged and recorded into the database as input for future analysis.

5.6 Guidelines on Acquiring New Information

Introduction

The modern world thrives on information and it is the driving force that now fuels society. It is crucial to many aspects of business and the life of the stakeholders and therefore should be managed well. This has also led to the evolution of using technology to store, process or transmit information through electronic means.

Scope

This section will provide general guidelines when acquiring information to conduct forensic analysis done by the CERT of the institution.

Target Audience

This section is intended for personnel who are:

- Assigned as Analyst tasked with gathering, collecting, searching, reviewing, and analyzing information security incidents that have been reported.
- Members of the CERT.
- Responsible for managing, supervising, and directing the members of the CERT.

a. Guidelines for handling e-discovery

- Adopt a process for reporting information relating to a probable threat of litigation to a responsible decision-maker to assist in demonstrating reasonableness and good faith;
- To determine the scope of information that should be preserved, it should be factored into the process of decision-making, the amount of information that should be preserved, the nature of the issues raised in the matter of information preservation, the accessibility of information, the probative value of information and the relative burdens and costs of preservation efforts;
- Compliance with a legal hold should be regularly monitored; and
- Any legal hold policy, procedure or practice should include provisions for releasing the hold upon the termination of the matter at issue so that the organization can adhere to

policies for managing information through its useful lifecycle in the absence of legal a hold.

- Ensure the e-discovery process aligns with the Electronic Commerce Act regarding the handling of electronic evidence

Chapter 6.0 General Procedures

Introduction

During the initial stage of the event, the process of decision-making is already in progress. The information gathered and collected will provide the basis to evaluate and assess the relevancy of information to initiate a series of responses to limit.

Scope

This section covers the procedures for the three stages of the computer emergency response plan of CERT.

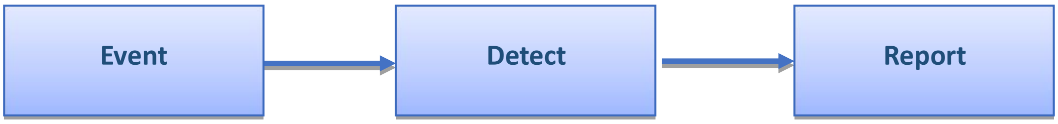
6.1 Detection and Reporting Procedure

Control Objectives

1. Gathering and collecting of information should be identified and evaluated for relevancy of information and made available to the users who need it.

2. Documentation and appropriate logging of records and data shall be maintained for regular monitoring and updating of the database.

Stages and Processes



a. Receiving Calls or Reports

1. All calls received are filtered and directed to appropriate personnel with specific CERT tasks and responsibilities.

2. All reported calls received are immediately logged into the system after it has been filtered as relevant security information events that will prompt the incident response team to initiate a series of processes and responses.

b. Detection of Event through Human Means

1. Use the Initial Assessment Form (IAF1) to gather and collect data for analysis of the relevancy of the information;

i. Given the potentially time-critical nature of the process; it is not essential to complete all fields in the reporting form at this time.

2. Fill the IAF1 with appropriate information and ensure the approximate time is recorded when the event was initially detected;

3. Ensure that the name of the person reporting (if, applicable), the name of the person gathering and collecting information and the person assigned to respond are indicated in the IAF1:

   - Initial assessment results with relevant information after initial evaluation of the CERT Analyst are assigned with Case Number and prompted for Second Assessment.
   - Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with responding to a security incident or event.
   - Case Numbers with open or unresolved status are reviewed and monitored closely to contain and control any other potential adverse impact.
   - Case Numbers with closed or resolved status are logged into the system to update the record.
   - Summary of resolved and unresolved cases are reported on a daily and weekly basis.

c. Detection of Event Through Automatic Means

1. Use IAF1 to gather and collect data for analysis of relevancy of the information;
2. Fill the IAF1 with appropriate information and ensure the approximate time is recorded when the event was initially detected;
3. System or network server clock is used as the official time when the event was initially detected;
4. Use IAF1 to gather and collect information for evaluation by the CERT Analyst;
5. Initial assessment results with relevant information after initial evaluation of the CERT Analyst are assigned with Case Number and prompted for the Final Assessment Form (FAF1);
6. Final assessment results considered to be relevant are forwarded to the appropriate personnel tasked and assigned with the roles of responding to a security incident or event;
7. Case Numbers with open or unresolved are reviewed and monitored closely to contain and control any other potential adverse impact;
8. Case Numbers with closed or resolved are logged into the system to update the record; and

9. Summary of resolved and unresolved cases are reported on a daily and weekly basis.

6.2 Assessment Decision Procedure

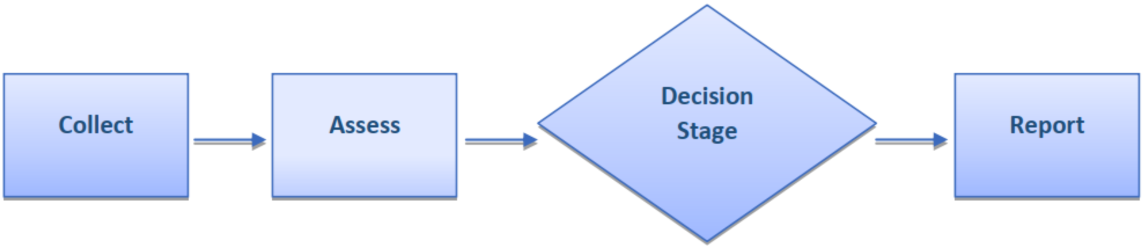
Control Objectives

1. Determine the type of detected and reported incident from false alarm and relevant.

2. Classify assessment results according to the degree of loss and the adverse impact it may cause the organization.

3. Submit interim reports for reported incidents that require longer periods of responses.

Stages and Processes



a. Initial Assessment and Decision

1. All completed information security event reporting forms are acknowledged by the receiving person;

2. All collected data and information are entered into the information security event/incident database;

3. All reports are reviewed after it has been logged into the system. Seek any clarification from the person reporting the information security event and collect any further information required and known to be available, whether from the reporting person or somewhere else;

4. Assessment is conducted to determine whether the information security event is a false alarm, a security incident, or a false alarm:

    - If the information security event is determined to be a false alarm, the information security event reporting should be completed and communicated to CERT for addition to the information security event/incident database and review, and copied to the reporting person and the manager under whom the person is assigned, concerning the time zone difference using Philippine Standard Time as reference point:

- If a reported information security incident or event is identified as local, a response from the reporter should be within 24 hours after it was initially reported.

- if a reported information security incident or event is identified as international, the response from the reporter should be within 48 hours after it was initially reported.

- If the information security event is determined to likely be an information security incident, and if the person assessing it has the appropriate level of competence, further assessment must be conducted; otherwise, it should be forwarded to the person with the appropriate skill level to respond to the reported information security incident.

5. When considering the potential or actual adverse effect of an information security incident on the business of an organization, the first step will be to consider which of several consequences is relevant:

   - For information considered to be relevant, the related categories found under the Classification of Security Incidents, should be used to establish the potential or actual impacts for entry into the information security incident report.

   - All reported information security incidents that are tagged as resolved include details of the safeguards that have been taken and any lessons learned (e.g. safeguards to be adopted to prevent recurrence or similar occurrences).

6. Reporting forms that have been completed are referred to the CERT for entry into the information security event/incident database and review;

7. Interim reports are submitted for investigations likely to be longer than one week;

8. The analyst assigned to assess the information security incident report must know when it is necessary to escalate matters to whom; and

9. Documented change control procedures are applied in all activities conducted and must be followed.

b. Final Assessment and Incident Confirmation

1. CERT is responsible for the confirmation or decision to categorize the information security event after the final assessment:

   - The information security incident reporting form must be acknowledged as soon as it has been received;

   - Enter the form into the information security even/incident database;

- Seek clarification from the POC or operations support group to gain more information regarding the incident reporting form;

- Review the reporting form content; and

- Collect any further information required and known to be available, whether from the POC, the person who completed the information security event reporting form, the operations support group or elsewhere:

    - If there is still a degree of uncertainty to the authenticity of the information security incident or the completeness of the information, the CERT should conduct an assessment to determine if the reported incident is real or is a false alarm;

    - If the reported information security event is determined to be a false alarm:

        - The information security report is completed and logged to update the database system for information security events/incidents and communicated to the CERT Team Leader.

        - Copies of the report should be sent to the POC, the CERT Team Leader, the reporting person and the local manager of the reporting person.

    - If the reported information security incident is determined to be real then further assessment should be conducted, involving other colleagues with appropriate set skills and confirm the following:

        - How the information security incident was caused, its adverse effects, what has been affected, the impact or potential impact, and an indication of its significance;

        - Attacks done deliberately by human technical methods and techniques, determine the depth of the infiltration into the institutional system, service and or network and the level of control the attacker was able to obtain, the data that has been accessed, and the software that has been copied, altered or destroyed by the attacker;

        - Attacks done deliberately through a human physical attack on any of the institutional information system, service and/or network hardware and/or physical location, the physical damage whether indirect or direct must be examined and confirmed including the physical access into the facilities;

- Information security incidents not directly caused by human actions, whether direct or indirect (e.g. physical access open because of fire), should be determined and confirmed;

- Review the state and progress of the information incident security incident that has been dealt with so far; and

- A review being conducted on the potential or actual adverse effects of the information security incident on the operations of the institution should be confirmed to determine which of several consequences is relevant, (Refer to Classification of Security Incidents).

6.3 Response Procedure

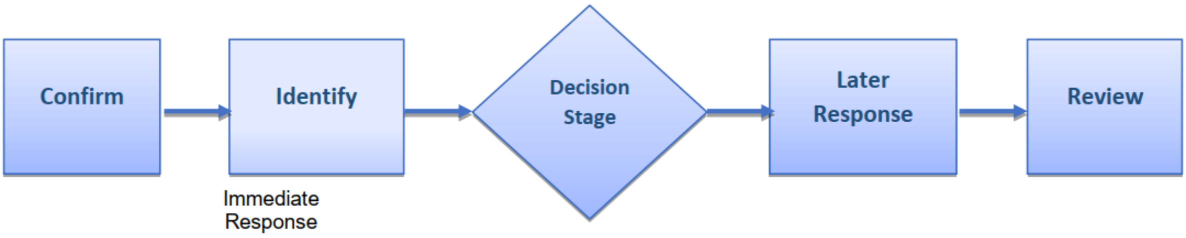
Control Objectives

- Confirm the assessment results on the relevant information to contain, minimize, or control the effects of the reported information security incident.

- Identify and execute immediate or later responses based on the situation

- Review of the responses (immediate or later), including the procedures, processes, and management system for responding to the information security incident

Stages and Processes



a. **Response**

- Identify Immediate response actions.
- Record details on the information security incident form and within the information security event/incident database;
- Notify appropriate persons or groups of the required actions.
- Initiate emergency and permanent safeguards to control or minimize the damage and impact of the reported information security incident;
- Determine the significance and severity of the information security incident report to CERT;
- Directly notify appropriate senior management when an information security incident is deemed significant or has been elevated to a crisis stage.

- Activate a business continuity plan if a “crisis” is evident and declared.

b. **Actions**

- Ensure critical applications and operations of the institution function correctly;
- Collect as much information as possible about the attacker;
- Implement appropriate authentication measures to prevent unauthorized individuals from accessing and attacking the system when emergency safeguards are called into action;
- Prioritize preventing recurrence, rectify the safeguard mechanisms through the exposed weaknesses of the attacker, and weigh the gains to justify the effort of tracking the attacker, especially when it is non-malicious and has caused little or no damage;
- Information security incident reports caused other than by deliberate attack must be investigated to determine the cause;
- Activation of surveillance techniques to counter the attacks of the hacker or attacker; and
- Check information that may be corrupted by the information security incident report against backup records for any modification, insertions or deletions of information,
- Check the integrity of the logs

c. **Incident Information Update**

- Always update the information security incident report as much as possible;
- Record and add updates to the information security event/incident database and notify the CERT Team Leader and others as necessary. Update includes:

  - What the information security incident is;
  - How it was caused and by what and whom;
  - What it affects or could affect the information system, operations and critical missions of the institution;
  - The impact or potential impact of the information security incident on the business and operations of the institution;
  - Changes to the indication as to whether the information security incident is deemed significant or not; and
  - Current state or progress of how the reported information security incident has been dealt with so far.

- If the reported information security incident has been resolved, the report includes details of the safeguards that have been taken and any other lesson learned;

- CERT is responsible for ensuring the secure retention of all information about an information security incident for further analysis and potential legal evidential use,

i. All volatile data are collected before the affected IT system, service or network is shut down for a complete forensic investigation which includes the following actions:

- Information to be collected includes contents of memories, cache and registers and details of any processes running;

- Full forensic duplication of the affected system, service and/or network, or a low-level backup of logs and important files;

- Collect and review logs from neighboring systems, services and networks such as routers and firewalls;

- Store all information collected on read-only media;

- At least two persons, while the forensic duplication is performed, must be present to assert and certify that all activities that have been carried out comply with the relevant legislation and regulation;

- Document the specifications and descriptions of the tools and commands used to perform the forensic duplication which must be stored together with the original media; and

- The CERT member should facilitate the return of the affected facility to a secure operational state that is not susceptible to compromise by the same attack.

d. **Other Activities for Reports Assessed as Significant**

- Institute forensic analysis procedure in compliant with legal requirements for evidence handling and privacy protection;

- Inform and coordinate with personnel responsible for internal and external communications of the facts and the proposals for what must be communicated in what form and to whom;

- Any information security incident report that has been completed must be entered into the database system for information security event/incident to update records;

- Interim reports must be instituted for investigations likely to have longer time to undertake;

- CERT members must observe and be made aware of the documentation requirements for the following:

  - The manner of necessity to escalate matters and to whom

- Change management
- The information security incident report shall be reported in the first instance to relevant people in person, by telephone or text messaging as a contingency plan for communication:
- Establish a secure method of communication
- Nominate backup advisors, deputies or representatives in the case of absence

e. **Incident Control**

- A review shall be conducted after immediate responses have been instigated to control the incident:

  - Consult with colleagues if necessary;
  - If the reported information security incident is confirmed to be under control, institute later responses, forensic analysis, and communications to close the reported incident and restore normal operations; and
  - If a reported information security incident is confirmed to be not under control, institute "crisis activities" to activate the crisis management plan.
  - Follow the Forensic Analysis for the detailed review process for immediate responses.

f. **Later Responses**

- Identify the "if and what" further responses are required to deal with the information security incident, including:

  - Restoring the affected information systems, services and or networks back to normal operations;
  - Recording details on the information security incident reporting form;
  - Updating the details and information report into the information security incident/event database; third-party
  - Notifying the personnel responsible for completing related actions;
  - Contacting supplier immediately if the institution relies on external vendors for hardware and software and other third-party support services;
  - Conducting additional monitoring activities after restoring to normal operations to detect other weaknesses or vulnerabilities; and
  - Conducting recovery activities when incidents were caused by non-IT-related causes.

g. **Crisis Activities**

- Institute crisis activities leading to the activation of a crisis management plan;
- Activate fire suppression facilities and evacuation procedures for fire-related incidents;

- Activate flood prevention facilities and evacuation procedures for flood-related incidents;
- Activate bomb “handling” and related evacuation procedures for bomb threat and domestic terrorism-related activities; and
- Activate procedures to put on board specialists such as information system fraud investigators and technical attack investigators for cyber-attacks and intrusion-related incidents.

h. **Forensic Analysis**

- Avoid having the target being rendered as unavailable, altered, or otherwise compromised by protecting the system, service and/or network during the forensic analysis procedure:
  - Protect against new viruses that may be introduced during the conduct of forensic analysis.
  - Minimize or no effects will be made on normal operations.
- Prioritize the capture of evidence by proceeding from the most volatile to the least volatile;
- Identify all relevant files on the subject systems, service, and/or network, including normal files, deleted files, password or password-protected files, and encrypted files:
- Recover discovered deleted files and other data:
  - Uncover IP addresses, hostnames, network routes and website information;
  - Extract contents of hidden, temporary, and swap files used by both the application and the operating system software;
  - Access the contents of protected or encrypted files unless it is a possible violation of a law;
  - Analyze all possible, relevant data found in special and typically inaccessible data and disc storage areas;
  - Analyze file access, modification and creation times;
  - Analyze system, service, network, and application logs;
  - Determine the activity of users and/or applications on a system, service or network;
  - Analyze emails for source information and content;
  - Perform file integrity checks to detect Trojan horse files and files not originally from the system;
  - If applicable, analyze physical evidence for possible fingerprints, property damage, video surveillance, alarm system logs, pass card access logs, biometric systems, and interview witnesses; and
  - Handle and store the extracted potential evidence by securing and protecting it from being

  - damaged or rendered unusable.

- Make sure that sensitive information and material cannot be seen by those not authorized to view recovered potential evidence;
- Evidence gathering must be in with accordance of the rules of the court or hearing, in which the evidence may be presented;
- Make conclusions on the reasons for the information security incident and the actions required including the timeframe. Provide a list of the evidence of relevant files to be included as attachments to main reports; and
- When required, provide expert support to any disciplinary or legal action that the institution will undertake.

i. **Communications**

- Prepare certain information in advance that can be quickly adjusted to the circumstances of a particular information security incident issued to the Media such as:

  - When a security incident is confirmed as real;
  - When a security incident is confirmed as under control;
  - When it is designated for “crisis” activities;
  - When it is resolved or closed; and
  - When post-incident review has been completed and conclusions reached.

- Prepare the personnel who will be tasked and assigned to communicate with internal (outside of normal CERT/management communication lines) and media;
- Information that is to be released must be according to the institution’s policy on information dissemination; and
- Information to be released must be reviewed by the relevant parties of the institution.

j. **Improve**

- Review the results of the forensic analysis that were further conducted after the information security incident report has been resolved and closure has been agreed;
- Conduct further forensic analysis to identify evidence even after the information security incident report form has been completed and viewed as closed or resolved. The same toolsets and procedures must be used for further forensic analysis of evidence;
- Identify the lessons to be learned once the information security incident has been concluded as closed or resolved, from the initial handling to quick

identification up to the level when immediate or later responses were taken. Lessons may include:

- New or changed requirements for information security safeguards, either technical or nontechnical safeguards which may include:
  - Rapid material updates;
  - Delivery of materials or support/shared services;
  - Security awareness briefings for end-users and personnel; and
  - Rapid revision and issue of security guidelines and/or standards.
    - Changes to the CERT and its processes, procedures, reporting forms, and information security event/incident database;
    - Look for patterns or trends beyond a single information security incident to help identify the need for safeguards or approach changes; and
    - Conduct information security testing and vulnerability assessment.

6.4 Responding to Information Security Report Procedure

Introduction

As part of establishing security for information technology, all employees, contractors, and third-party users must be made aware of the established procedures for reporting different types of events and weaknesses that might impact the security of institutional assets. Early reporting upon detection will ensure that information security events and weaknesses associated with the information systems of the institution are communicated promptly, allowing CERT to take timely corrective actions. CERT is tasked with responding to any reported information security event quickly, effectively and orderly to mitigate, prevent, minimize, control, or correct any vulnerabilities or threats that may adversely impact the organization.

Scope

This section covers the response procedure of the CERT.

Control Objectives

- Log and record all activities undertaken when responding to the information security incident
- Review established procedures to determine applicability and for continuous improvement of the institution’s information security incident response processes, procedures, and policies.
  - Responding to Information Security Incident Report
    - Use Form IAF1 and FAF1 as references when responding to reported incidents or events associated with the information system of the institution.

- Refer to the guidelines for handling incident response.

- Procedures for Responding to Different Types of Information Security Incident

  - When responding to information system failures and loss of service:

    - Immediately halt attacks if caught while in progress;
    - Follow backup procedures;
    - Assess the extent of operational downtime and determine the earliest time possible to bring the system into a stable operating state;
    - Check if data or information has been compromised or a security breach has occurred during a system failure or loss of service;
    - Check records of updates and regular maintenance being conducted such as version of the anti-virus software, installation or updates of patches to correct software vulnerabilities, firewall technology in place, etc.;
    - Review and monitor systems and determine the effectiveness of information security safeguards to detect and correct the breakdowns in security. Monitoring and review may include:

      - Sampling
      - System checks
      - Reports of access to systems
      - Review of Logs
      - Audit Reports

- Preserve and gather evidence that results from the incident that has occurred;
- In an urgent situation that requires immediate action please refer to the established escalation procedure,

  - The CERT member responding is authorized to secure the asset without the owner’s consent when it is determined to be critical:

    - Appropriate logging and recording of artefacts must be conducted.

    - Another member of the CERT must be present or a representative from the reporting party must be around to observe the secure removal of the item from the site.

  - When responding to malicious code attacks

    - Determine fully if a malicious code attack has occurred, evaluated based on some of the examples below:

- Complaints on slow access to internet, exhaustion of system resources, slow disk access or slow system boots;
- Numerous alert reports have been generated by Host-based Intrusion Detection System (HID) or by anti-virus or malicious code detection software;
- Significance in increased network usage;
- Access violation entries are noticed and observed in perimeter router logs or firewall logs;
- A detected surge on out-bounced SMTP traffic originating from an internal IP address;
- Noticeable unusual deviation from typical network traffic flows observed by a system administrator;
- Security controls such as anti-virus software and personnel firewalls are disabled on many hosts; and
- General system instability and crashes.

- Upon confirmation of a malicious code security breach, collect information about the malicious code;

- Identify characteristics of the malicious code to apply the appropriate course of action. Examples are given below:

    - Type of malicious code: network mass, mass-mailing worm, virus, Trojan horse, etc.

    - Vulnerability that is being exploited by the malicious code, services or ports being attacked, etc.

- Assess the scope, damage and impact of the outbreak to effectively deal with the incident;

    - Record all actions taken when dealing with the outbreak and any corresponding results, (Please see General Procedures for Phase 2). Logging should be carried out throughout the whole security incident response process;

    - Notify all appropriate parties and escalate the incident to the appropriate level following a predefined escalation procedure (Please see Escalation Procedure). The information provided during the escalation process should be clear, concise, accurate and factual. Inaccurate, misleading or incomplete information may hinder the response process or may even worsen the situation; and

- Carry out containment activities to prevent the malicious code from inflicting further damage through the following:

    - Identify infected systems;

    - Contain the outbreak;
    - Keep a record of all actions taken;
    - Execute the full eradication process as soon as possible or in parallel with the containment process to prevent files from being corrupted, destroyed or deleted on the infected system.
    - Notify all related parties before the resumption of suspended services. IT personnel must restore specific functions and servers' stage by stage in a controlled manner and in the order of demand. Start with the most essential services or those servicing the majority.
    - Verify information that the restoration operation has been successful and that all services are back to normal after resuming the suspended services. Additional monitoring may be implemented to watch and observe for any suspicious activity in the network segments concerned.

  - When responding to Distributed Denial of Service (DDoS)

    - Immediately assess and determine the scope and impact to plan for the next course of action to address the incident.
    - Determine the intent, capability, and target of the attacker to deploy appropriate countermeasures and install safeguard mechanisms,
    - Ensure additional components are immediately available as replacements in the event of component failure,
    - Use load balancing mechanisms to distribute the force of DDoS attacks between several components and geographic locations to prevent a single component or network from receiving the full volume of traffic,
    - Immediately execute the escalation procedure,

- Ensure appropriate physical security measures are in place to detect unauthorized entry or access into the site,
- Immediately detect or remove reflectors or amplifiers from the network to minimize avenues of anonymity and large-scale assaults on the system, as well as lower the risk for critical infrastructure of the organization,

    - When responding to breaches of confidentiality and integrity

- Immediately assess the impact and the degree of security breach,
- Implement escalation procedure immediately,
- Review all logs and records of entry and exit of all personnel with access to critical information systems and data processing facilities including data storage facilities,
- Change all passwords and entry codes immediately,

- Record all activities taken for further analysis and improvement of the security systems being implemented,

  - When responding to misuse of information system

- Trace logs and records of all transactions,
- Execute control measures immediately to further prevent any unauthorized access,
- Investigate and evaluate the intent and extent of the impact of the misuse of the information system,
- Change all passwords and entry codes immediately,
- Review implementation of security password maintenance, security logs, and security access into the system,
- Immediately disconnect the equipment or remove it from the network connection when unauthorized use or access of the information system has been detected and confirmed,
- Record all activities taken for further analysis and improvement of the security systems being implemented.

6.5 Reporting Procedure

Introduction

When an information security event is detected whether by human or automated means, and reported immediately, it increases the ability of the CERT to verify the information and initiate an immediate response when it has been determined to be relevant. The person tasked with receiving all reported information security incidents must be able to report and notify appropriate personnel. The process of reporting a security information incident is not only limited to reporting the initial event but Also involves knowing how to escalate the incident to the next level of decision-makers when necessary.

Scope

This section covers the reporting procedure upon the initial receipt of a report of an information security event or incident, interim reporting and escalated reporting.

Control Objectives

- Acknowledgment receipt of the information security incident report
- Recording of the official time stamp of the information security event upon initial report
- Forms for the following: IAF1 and FAF1

a. Initial Reporting of Information Security Incident Report

- All calls are filtered by the POC to determine if the call is related to a report on an information security incident.

- The initial incoming report on information security incident is logged into the system to record and log report into the database for information incident/event database,

- Initial information from the incoming calls or reports is recorded into the IAF1.

- The IAF1 with partial information is forwarded to the CERT Analyst for data gathering and collection.

- The Initial Report is forwarded to the concerned personnel for immediate response and the CERT Team Leader is informed.

- All reports must be updated when it has been closed or resolved to update the system.

6.6 Escalation Procedure

Introduction

Escalation occurs when circumstances require matters to be escalated to the top management, another group, or persons within the institution or groups outside the institution. However, it is important that before the incident is escalated, ~~a~~ll means to respond immediately to the incident are exhausted, or it qualifies as an urgent matter that can affect institutional security.

Scope

This section will cover procedures for escalation, including when, what and who to notify about a matter that is being escalated.

Control Objectives

- Assessment reports to determine the relevance of the reported information security incident;
- Impact and risk assessment reports that will initiate the decision to escalate matters;
- Rating scale for vulnerability, threat, and predisposing conditions to support and justify the action to escalate; and
- Escalation request form that will provide a paper trail for auditing.

a. **Factor to Consider for Escalation**

- When results of the evaluation are determined to have an impact to the institutional security:

    - When the results of the evaluation have a severe or catastrophic adverse impact on the institution;

    - When the results of the evaluation will be classified as critical and will severely affect the information system level of the organization;

- When major issues become evident at the early stages of reporting; and
- When an information security incident report is a recurring incident after it has been previously resolved.

b. **Escalation Procedure**

- Use the rating scale on vulnerabilities and threats to evaluate the degree or gravity of adverse impact on the institution;
- The decision to escalate will be taken by the CERT Leader after determining the results of the evaluation;
- Escalation requests must include the following:
  - The type of event and when it happened;
  - The degree of severity or adverse impact to the institutional level or the information system level;
  - The name of the person requesting for escalation and the official time stamp and date when escalation requests were made; and
  - The case number assigned to the information security incident report.
  - The Analyst shall consult with the Team Leader when major issues are evident during the early stage of assessment;
  - Send an alert message notifying the appropriate personnel to respond to the escalated information security incident report;
  - The Analyst shall consult with the Team Leader when the reported information security incident is required for escalation;
  - The Analyst shall consult with the Team Leader to determine the next course of action whether it should be escalated or forwarded to another group to initiate an immediate response or take a series of actions;
  - Notification of escalation after assessment results are concluded and Escalation Request is forwarded and submitted to the Team Leader;
  - Escalating the information security incident report must have supporting documents that will justify and rationalize the escalation requests;
  - All escalated information security incident reports must be monitored at regular intervals to ensure that it has been properly coordinated and forwarded to the personnel concerned;
  - Escalated information security incident reports must be logged into the system to update the information security event/incident database; and
  - A summary of the escalated report on information security incidents must be prepared and submitted to the CERT Team Leader for review and evaluation.

c. **De-escalation Procedure**

- When the escalated information security incident report is addressed and its classification has been downgraded to a manageable and controllable incident, a de-escalation notification is forwarded to:

  - The source where the report has emanated
  - The Reporting Analyst
  - The CERT Team Leader
  - The CERT Supervisor
  - The CERT

- When the escalation request is reviewed and evaluated to determine the impact and severity and is concluded to be manageable, controllable and within the scope of an existing set of skills of the CERT Team, the escalation notification request will be downgraded and forwarded to the concerned personnel with the specific set skills to respond immediately or for later responses.

- De-escalated information security incident reports must be logged into the system to update the information security event/incident database.

6.7 Communication Procedure

Introduction

When an information security incident occurs, there are instances when the need to communicate and coordinate with other groups or third parties is very important. Whenever appropriate, such as contacting law enforcement agencies, responding to media inquiries or discussing and sharing information with ISPs and vendors of vulnerable software or other incident response teams, the need to establish policies and procedures to ensure that sensitive information is not disclosed to unauthorized parties is required. This prevents potentially leading to additional disruption, reputation damage, or financial loss. Any communication conducted with outside parties must be well documented for evidentiary and liability purposes.

Scope

This section covers communication procedures with outside parties or external groups during incident response.

Control Objectives

1. Communication policies are developed to ensure that sensitive or critical information is not disclosed when communicating and coordinating with parties and groups outside CERT.

2. Record of communication activities are documented and must be stored and filed in a secure place.

a. Media Communications Procedure

- All members of CERT must be oriented and trained on how to interact with media regarding incidents. Included are as follows:
  - Emphasis on the importance of not revealing important information such as technical details of countermeasures that could assist other attackers;
  - Discuss positive aspects of communicating and disclosing important information to the public fully and effectively;
  - Hold mock interviews and press conferences to simulate media interaction during incident handling;
  - A single POC person must be appointed and tasked to respond to handle the media and inquiries;
  - Disclosure of information must have written approval from the Top Management to ensure protection of information security;
  - All communication with outside parties must be documented accordingly; and
  - Media communications procedure must be reviewed at regular intervals to determine its applicability, and effectiveness and establish continuous improvement.

b. Contacting and Communicating with Law Enforcement Procedure

- Whenever the situation requires contacting law enforcement agencies, this must be established immediately.
- Communicating and sharing information with law enforcement agencies must be with written approval from the Top Management.
- Establish a single POC with the NPC or DICT or secure alternate contact persons to ensure availability when the need to communicate and coordinate with the agency arises.
- All communication and coordination activities are recorded and documented accordingly.

c. Contacting Other Groups

- Communicating and contacting other groups while responding to information security incidents must be with written approval from the institution.

- A single POC is assigned to have all communication directed and handled during incident response.

- All contact details from external groups are updated and distributed to the CERT member responding to the incident response.

- The CERT Supervisor must monitor all communication activities.

- Record and document all communication with external groups or third parties accordingly.

- Review records of communication at regular intervals to evaluate the procedures and processes for conducting communication with other parties outside CERT.

6.8 Review Procedure

Introduction

The review stage is an important process to ensure that the established incident response system of the institution is working efficiently and effectively. It is also a chance for CERT to analyze and evaluate lessons that can be learned from the data gathered and collected including the related responses and associated decisions undertaken during initial and post-incident activities. The review stage provides the avenue to also monitor all unresolved including resolved cases to evaluate the recommendations provided during incident response.

Scope

This section covers the review procedures that are conducted by the CERT as part of the objective for continuous improvement.

Control Objectives

1. Post-incident reviews are conducted to determine the efficiency of the processes and procedures established for the CERT.

2. Outputs of the reviews and their corresponding results are used as input for refining the processes and procedures of CERT.

3. Review outputs are documented for evidentiary purposes.

a. Review Procedures

- All records and documented activities for incident responses are reviewed at regular intervals.

- A monthly meeting with the CERT is scheduled to review all post-incident reports that were resolved immediately during the initial response and are summarized for discussion.
- For incident reports requiring a longer period of investigation, schedules for meetings are conducted with more frequency to ensure that all response activities are monitored and reviewed.
- All post-incident reports that took longer time to be resolved are reviewed and evaluated further to gather lessons to be learned:

    - Develop a knowledge database of best practices from lessons learned;

    - Develop a knowledge database for research and development;

    - Consolidate the knowledge database for the latest techniques, approaches and methods for incident response;

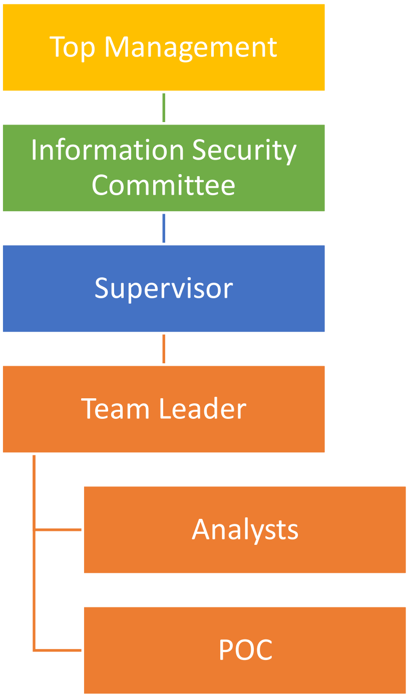
    - All communication and coordination activities must be reviewed to improve the procedures and processes when communicating outside CERT;

    - Results of review meetings and discussions are reviewed during the next scheduled meeting; and

    - All reviews are documented and records are submitted to ASSCCAT.

Annex A

Organizational Structure



Annex B

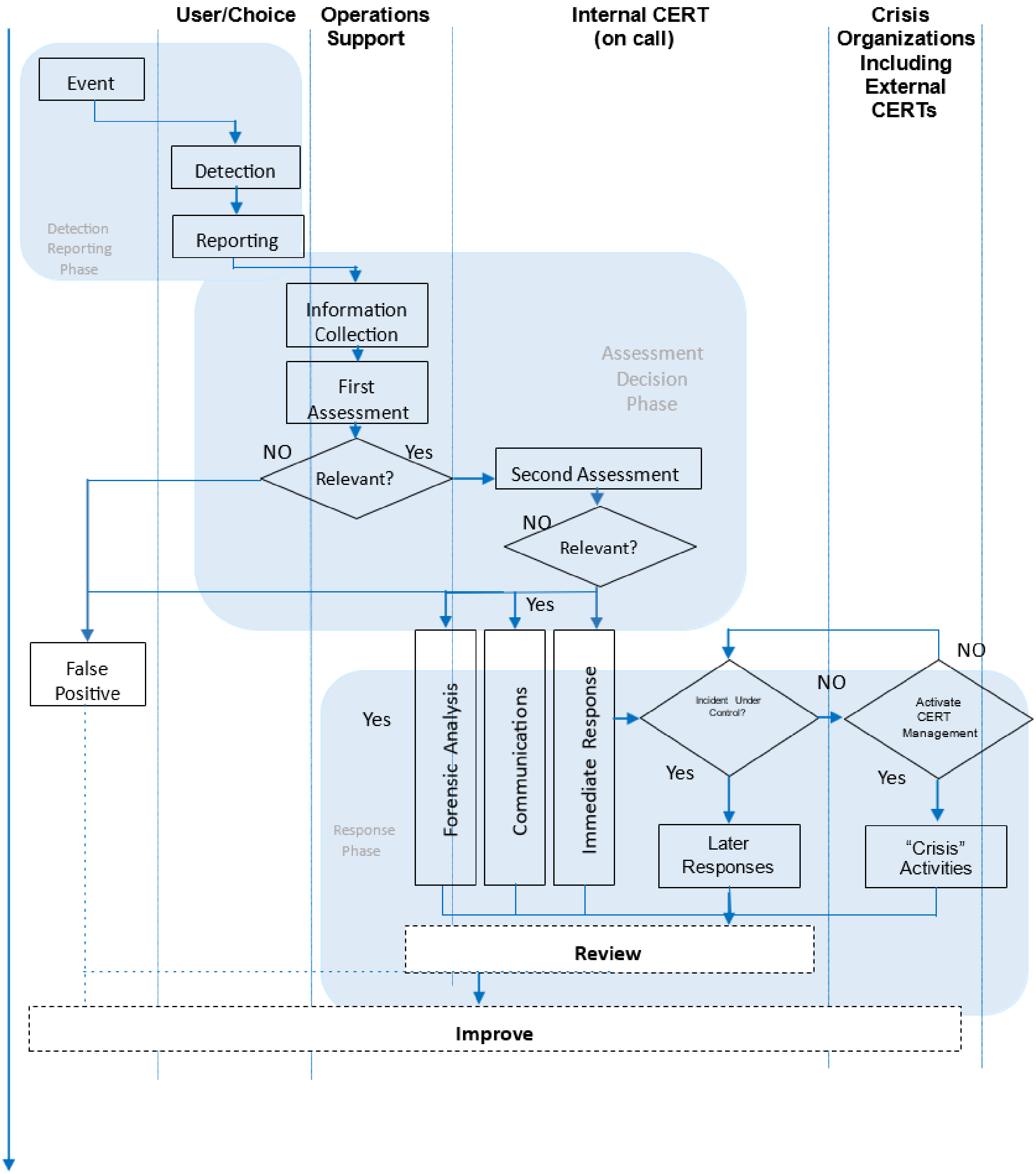
Skills and Competency Framework

Level	Position	Set Skills	Competency	Mastery or Expertise
1	POC	Computer literate, communication skills, encoding, probing techniques, basic knowledge of OS, active listening skills, listening comprehension skills	Customer service management, critical thinking skills, analytical thinking skills, general administrative skills, multi-tasking ability	Conflict resolution management skills, public relations and communications skills
2	Analyst and Team Leader	Advanced computer knowledge, technical and report writing, interpersonal and intrapersonal skills, advanced probing technique, time and task management	Leadership skills, supervisory and management skills, planning and execution skills, basic project management skills, ability to conduct forensics based on existing standards, problem-solving and decision-making skills, high degree in mathematical and logical thinking ability, team motivation ability	Advanced digital forensic investigation, a wide range of knowledge on various types of hardware platforms, coaching and mentoring skills, training skills, mastery of computer forensic best practices and industry-standard methodologies for acquiring and handling digital evidence, advanced technical understanding of digital forensic principles and

Level	Position	Set Skills	Competency	Mastery or Expertise
				techniques, solid knowledge on laws and regulation related to ICT and computer
3	Supervisor	Digital forensics skills, advanced computer forensic hardware and computer knowledge, MS Windows, Unix-like or mobile phone operating systems, negotiating skills with decision makers and executives, extensive knowledge of laws and regulation related to ICT and computer	Leadership skills, mentoring and coaching skills, training skills, conflict resolution management skills, team building development, planning skills, supervisory and managerial skills, advanced project management skills, problem solving and decision-making skills, mathematically inclined with logical thinking ability	Superior knowledge of computer forensic best practices and industry standard methodologies for acquiring and handling digital evidence, superior technical understanding of digital forensic principles and techniques

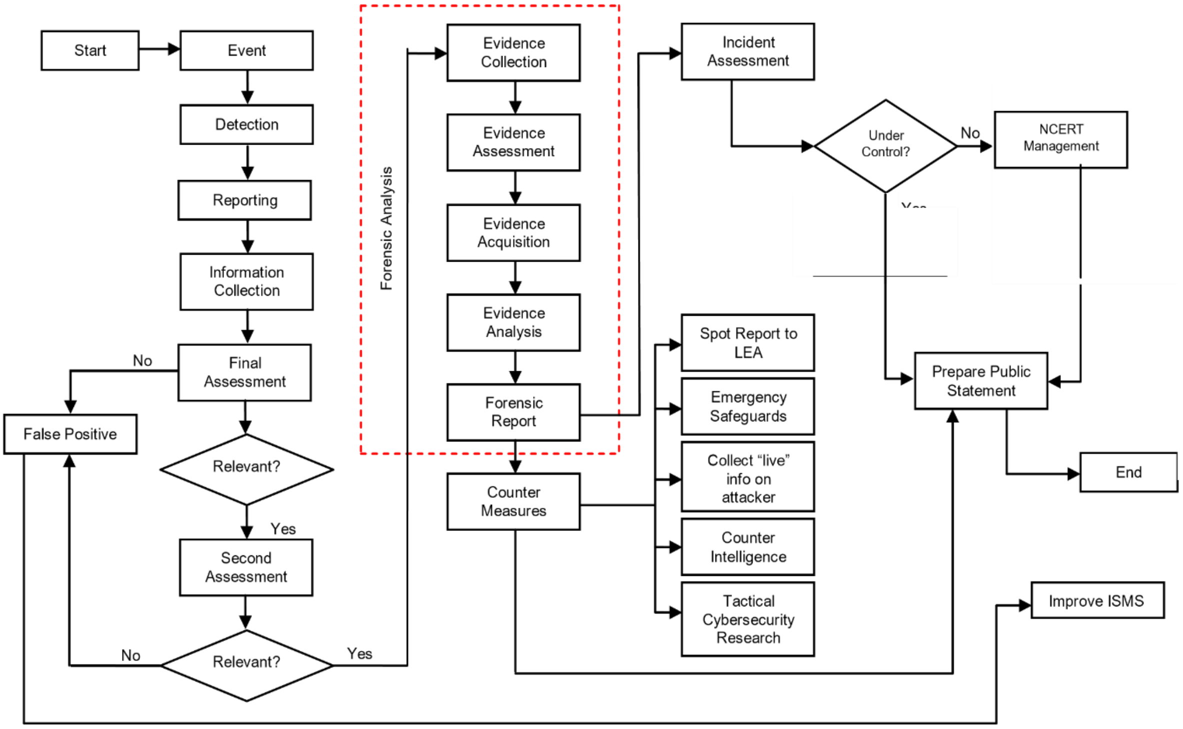
ANNEX C

Computer Emergency Response Team (CERT) Key Processes



ANNEX D

Flowchart for Incident Handling Responses



Prepared by:

IRENE C. BALUIS
Chief Information Security Officer
Information Technology Officer I

Approved by:

JOY C. CAPISTRANO, Ph.D.
College President