	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

## TABLE OF CONTENTS

1.0	INTRODUCTION .....	3
1.1	PURPOSE AND OBJECTIVES .....	3
1.2	SCOPE .....	3
2.0	RELATED DOCUMENTS .....	3
3.0	ORGANIZATION OF THIS POLICY .....	4
4.0	INFORMATION SECURITY POLICIES .....	4
4.1	MANAGEMENT DIRECTION FOR INFORMATION SECURITY .....	4
5.0	ORGANIZATION OF INFORMATION SECURITY .....	4
5.1	INTERNAL ORGANIZATION .....	4
6.0	USER SECURITY .....	4
6.1	PRIOR TO EMPLOYMENT OF EMPLOYEES/ ENGAGEMENT OF PERSONNEL AND THIRD PARTY CONTRACTORS .....	4
6.2	DURING EMPLOYMENT/ ENGAGEMENT .....	5
6.3	TERMINATION AND CHANGE OF EMPLOYMENT/ ENGAGEMENT .....	5
7.0	ASSET MANAGEMENT .....	5
7.1	RESPONSIBILITY FOR ASSETS .....	5
7.2	DATA CLASSIFICATION .....	5
7.3	MEDIA HANDLING .....	5
8.0	ACCESS CONTROL ( <i>Refer to Standard on Controlling Access to Information and Systems for the details.</i> ).....	6
8.1	ACCESS CONTROL .....	6
8.2	USER ACCESS MANAGEMENT .....	6
8.3	USER RESPONSIBILITIES .....	6
8.4	SYSTEM AND APPLICATION ACCESS CONTROL .....	6
9.0	CRYPTOGRAPHY .....	6
9.1	CRYPTOGRAPHIC CONTROLS .....	6
10.0	PHYSICAL AND ENVIRONMENTAL SECURITY .....	6
10.1	SECURE AREA .....	6
10.2	EQUIPMENT SECURITY .....	7




**INFORMATION SECURITY**

Information Technology Division

**Information Security Policies**

Prepared By	Information Technology		
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

- 11.0 OPERATIONS MANAGEMENT..... 7
  - 11.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES..... 7
  - 11.2 PROTECTION FROM MALWARE ..... 7
  - 11.3 BACK-UP ..... 7
  - 11.4 LOGGING AND MONITORING ..... 7
  - 11.5 CONTROL OF OPERATIONAL SOFTWARE ..... 7
  - 11.6 VULNERABILITY MANAGEMENT ..... 7
  - 11.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS..... 8
- 12.0 COMMUNICATIONS SECURITY ..... 8
  - 12.1 NETWORK SECURITY MANAGEMENT ..... 8
  - 12.2 INFORMATION SECURITY TRANSFER ..... 8
  - 12.3 MOBILE DEVICE MANAGEMENT ..... 8
- 13.0 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE ..... 8
  - 13.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS ..... 8
  - 13.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES ..... 8
  - 13.3 USING LIVE TEST DATA..... 8
- 14.0 SUPPLIER MANAGEMENT (*Refer to Third Party Partner Management Standards*) ..... 8
  - 14.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS ..... 8
  - 14.2 SUPPLIER SERVICE DELIVERY MANAGEMENT ..... 8
- 15.0 INFORMATION SECURITY INCIDENT MANAGEMENT..... 9
  - 15.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS ..... 9
- 16.0 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY (*Refer to Standards on Planning for Business Continuity for the details. – WIP\**) ..... 9
  - 16.1 INFORMATION SECURITY CONTINUITY ..... 9
  - 16.2 FACILITIES REDUNDANCIES ..... 9
- 17.0 COMPLIANCE..... 9
  - 17.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS ..... 9
  - 17.2 INFORMATION SECURITY REVIEWS ..... 9

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

## INFORMATION SECURITY POLICIES

### 1.0 INTRODUCTION

The Company (i.e. ABS-CBN Corporation and the subsidiaries who will adopt this policy) recognizes the role of Information Security in ensuring confidentiality, integrity and availability of information. Any risk or challenge to information security can affect and damage the Company’s operations, reputation and cause financial loss. To eliminate, or at the very least minimize and mitigate, these risks, Information Security Management shall be an integral part of the Company’s overall management system to establish, implement, monitor, review, maintain and improve information security.

### 1.1 PURPOSE AND OBJECTIVES

The overall objective of the General Information Security Policy is to establish mandatory requirements for the Company in securing all forms of information (e.g. computer data, documentation, intellectual property, etc.).

This Policy aims to protect the security of IT Resources to ensure that:

1. confidentiality is not breached, i.e. information is accessed only by authorized users;
2. the integrity of information is maintained, preserving its accuracy, currency and appropriateness;
3. information is always available to those who need it;
4. the Company complies with legal and regulatory requirements; and
5. the reputation of the Company is upheld.

### 1.2 SCOPE

The General Information Security Policy (the “Policy”) covers all of the Company’s IT Resources. Further, this Policy is applicable to all Company data and information, regardless of format and platform used, now existing and hereinafter developed.

This Policy applies to all users who create, use and access the Company’s IT Resources, regardless of location and manner of access. Unless otherwise provided in other policies, the following users are covered by the Policy:

1. Employees<sup>1</sup>
2. Personnel engaged by the Company to render services (e.g. Intellectual Property Creators (IPC), Independent Contractors (IC)<sup>2</sup>, On the Job Trainees, etc.)
3. Third Party Contractors (e.g. Vendors, Suppliers, agency personnel, etc.)


### 2.0 RELATED DOCUMENTS

The following documents are related to the General Information Security Policy:

1. ABS-CBN Code of Conduct (HR Division)
2. On-Boarding and Off-Boarding Policy (HR Division)
3. Security Policy (Corporate Security & Safety Division)
4. Asset Management Policy (Asset Management Division)
5. Audit Policy (Internal Audit Division)
6. Procurement Policy (Procurement Division)

<sup>1</sup> Refers to all employees of the Company, whether regular (union and non-union members), probationary, project, contractual or casual employee, regardless of rank or position level, program/ workpool employees. *[Definition lifted from ABS-CBN COC]*

<sup>2</sup> For IPCs and ICs, extent of coverage to Information Security Policies shall be based on the terms of their Contract.

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

7. Vendor Management Policy (Procurement Division)
8. IT Service Management Policy

### 3.0 ORGANIZATION OF THIS POLICY

This document outlines the General Information Security Policy and is aligned to ISO/IEC 27001:2013: Information Security Management System, covering the Company’s management direction (5.0), organization (6.0), user (7.0), asset management (8.0), access control (9.0), cryptography (10.0), physical and environmental security (11.0), operations security (12.0), communications security (13.0), systems acquisition, development and maintenance (14.0), supplier relationships (15.0), information security (16.0), business continuity (17.0), compliance (19.0), review and enforcement.

Standards, guidelines and procedures of these control areas shall be defined in separate documents.

### 4.0 INFORMATION SECURITY POLICIES

#### 4.1 MANAGEMENT DIRECTION FOR INFORMATION SECURITY

The Company is committed to implement security controls that follow the best practices, as set out in the ISO/IEC 27001:2013: Information Security Management System. The Company shall define specific Information Security standards, procedures and guidelines in order to ensure the confidentiality, integrity and availability of its information.

### 5.0 ORGANIZATION OF INFORMATION SECURITY

#### 5.1 INTERNAL ORGANIZATION

Information Security, under the office of the Chief Technology Officer, shall oversee the development, implementation, compliance with, and maintenance of a Company-wide Information Security Management System and Information Security Policy. It shall work with individuals and departments to deliver policies, standards, guidelines, procedures and solutions and to operate activities compliant with the Information Security Systems Plan and the Information Security Policy.

Information Security shall advise the Company on information security-related risk issues and, in consultation with other IT service owners, recommend appropriate actions in support of the Company’s larger risk management program. It shall ensure appropriate risk mitigation and control processes to prevent or remediate security incidents as required.


Information Security shall provide sufficient education and training to users, as deemed necessary, to ensure they understand the importance of information security. It will also provide guidance to the Company to raise awareness, develop understanding and good practices and minimize risk of information security-related incidents.

Information Security shall establish and maintain appropriate contacts with relevant law enforcement authorities, regulatory bodies, and third parties with respect to this Policy.

Information Security will work with Internal Audit and engage third party services, as deemed necessary, to provide assurance of compliance with these policies.

### 6.0 USER SECURITY

#### 6.1 PRIOR TO EMPLOYMENT OF EMPLOYEES/ ENGAGEMENT OF PERSONNEL AND THIRD PARTY

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

## CONTRACTORS

Security responsibilities shall be taken into account when recruiting Employees, Personnel engaged by the Company to render services and Third Party Contractors (e.g. through adequate job descriptions, pre-employment screening and background check, etc.). Non-disclosure agreements and other information security related clauses shall be included in the relevant contracts (e.g. terms and conditions of employment contract, IPC, IC, or OJT contract, or Service Agreement, and other signed agreements on security roles and responsibilities) prior to employment, or to engagement.

### 6.2 DURING EMPLOYMENT/ ENGAGEMENT

All users of information shall be given appropriate training, as deemed necessary, and regular updates on information security policies. They shall be educated on the security requirements, security controls, legal responsibilities and proper use of IT Resources to ensure that they are informed of security threats/ vulnerabilities and to equip them to comply with the information security policy of the Company. It is the responsibility of the Immediate Superiors, or their respective agencies or employers, to track and ensure that the users are aware of and comply with this Policy. *(Refer to Standards on Delivering and Training User Awareness for the details. – WIP\*)*

All users shall have annual recertification, as deemed necessary, of the Acceptable Use Policy.

### 6.3 TERMINATION AND CHANGE OF EMPLOYMENT/ ENGAGEMENT

Immediate Superiors, or their respective agencies or employers, shall ensure that the security aspects of a user's exit from the Company or significant changes of roles shall be processed according to established procedures (e.g. returning corporate information and equipment in his possession, updating his access rights, and reminding him of his ongoing obligations under privacy laws, contractual terms, etc.).

## 7.0 ASSET MANAGEMENT

### 7.1 RESPONSIBILITY FOR ASSETS

All IT Resources shall be inventoried. IT shall ensure protection of these assets based on up-to-date industry standards.

Data/ Information Owners and Users shall be identified to be held accountable for the incidents and liabilities arising from non-acceptable use of these assets' security. *(Refer to Acceptable Use of IT Resources for the details.)*


### 7.2 DATA CLASSIFICATION

All Company information and data shall be classified to indicate the need, priority, criticality and degree of protection needed. An information classification system shall be used by the Company to define an appropriate set of protection levels and communicate the need for special handling measures. *(Refer to Data Classification Standards for the details. – WIP\*<sup>1</sup>)*

### 7.3 MEDIA HANDLING

Appropriate measures shall be implemented to manage the flow of Company information or document throughout its lifecycle – from creation, initial storage and use up to obsolescence and deletion or disposal. Information storage media shall be processed, managed, controlled and transported in such a way that the

<sup>1</sup> WIP: Work in Progress

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

information content is not compromised. Information shall be destroyed prior to storage media being disposed of or re-used. *(Refer to Standards on Processing Information and Documents for the details. – WIP\*)*

## **8.0 ACCESS CONTROL** *(Refer to Standard on Controlling Access to Information and Systems for the details.)*

### **8.1 ACCESS CONTROL**

Physical and logical access controls to Company information shall be implemented, but not limited to, the following: operating systems, applications, workstations and mobile devices connecting to the company network, databases and servers, and network levels.

### **8.2 USER ACCESS MANAGEMENT**

Provisioning of access rights to users shall be controlled from initial user registration to removal of access rights when no longer required, including special restrictions for privileged access rights. Management of access rights and authentication and regular reviews, audit and updates of access rights shall be enforced by the Authorized Group.

Immediate Superiors shall ensure that the appropriate departments are informed of the changes on a user's roles and responsibilities.

### **8.3 USER RESPONSIBILITIES**

Users shall be responsible for maintaining appropriate access controls on their workstations and all equipment and devices they are assigned to (e.g. choosing strong passwords and keeping them confidential).

### **8.4 SYSTEM AND APPLICATION ACCESS CONTROL**

Access to Company information shall be restricted (e.g. through secure log-on, password management, control over privileged utilities, restricted access to program source code, etc.).

## **9.0 CRYPTOGRAPHY**

### **9.1 CRYPTOGRAPHIC CONTROLS**


Use of encryption, cryptographic authentication and integrity controls (e.g. digital signatures and message authentication codes, and cryptographic key management) shall be implemented according to data classification. *(Refer to Data Encryption Standards and Data Classification Standards for the details.)*

## **10.0 PHYSICAL AND ENVIRONMENTAL SECURITY**

### **10.1 SECURE AREA**

IT Resources containing Confidential Data (e.g. data centers, server rooms, etc.) shall be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls, and physically protected from unauthorized access, damage and interference. The protection provided shall be commensurate with the identified data classification, risks and protection standards set by Information Security. The overall physical security within company sites shall follow the standards promulgated by the Physical Security Department of Corporate Security and Safety Division (CSSD). *(Refer to Access to IT Rooms Standards for the details.)*

Protection against fires, floods, earthquakes, bombs and other physical threats shall be properly designed, implemented and maintained in compliance with the Fire Code of the Philippines.

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

## 10.2 EQUIPMENT SECURITY

All equipment containing Company information shall be stored and maintained in a controlled environment. These equipment shall be checked to ensure compatibility with other information processing and security facilities of the Company.

These equipment shall not be taken off-site unless authorized, and shall be adequately protected both on and off-site. *(Refer to Standards on Securing Hardware, Peripherals and Other Equipment for the details. – WIP\*)*

Protection against unauthorized physical access shall result from the application of principles of security design and shall include the employment of technologies that support a security strategy of Deter, Delay, Detect and Rapid Response.

## 11.0 OPERATIONS MANAGEMENT

### 11.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES

All information security operating responsibilities and procedures shall be documented and implemented. Separate environments for development, testing and production shall be in place. *(Refer to Software Development Policy for the details.)*

All changes to production environment systems shall be controlled. *(Refer to Change Management Standards for the details.)*

Capacity and performance shall be managed.

### 11.2 PROTECTION FROM MALWARE

Up-to-date protection from malware (e.g. worms, viruses, etc.) shall be enforced.

### 11.3 BACK-UP

Appropriate backups shall be taken and retained based on regulatory and business requirements. *(Refer to Back-up and Recovery Standards for the details.)*

### 11.4 LOGGING AND MONITORING


System user, administrator and operator activities, exceptions, faults and information security events shall be logged and protected by safeguarding the integrity of the logs from tampering or deletion.

### 11.5 CONTROL OF OPERATIONAL SOFTWARE

Software installed on operational systems shall be controlled, kept up-to-date and shall include standard security features. *(Refer to Standards on Purchasing and Maintaining Commercial Software for the details. – WIP\*)*

### 11.6 VULNERABILITY MANAGEMENT

Vulnerability management shall be implemented to remove and mitigate the risks to the Company's information systems.

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

**11.7 INFORMATION SYSTEMS AUDIT CONSIDERATIONS**

IT audits shall be planned and controlled to minimize adverse effects on production systems and to avoid unauthorized information access.

**12.0 COMMUNICATIONS SECURITY**

**12.1 NETWORK SECURITY MANAGEMENT**

All Company networks and their associated services shall be secured. Appropriate segregation of network access shall be implemented.

**12.2 INFORMATION SECURITY TRANSFER**

Non-disclosure and confidentiality concerning information transfer to and from third parties, including electronic messaging and verbal communications, shall be agreed and signed.

**12.3 MOBILE DEVICE MANAGEMENT**

Security of mobile devices (e.g. laptops, removable media, smartphones, etc. connecting to Company resources), remote and virtual workplaces shall be managed, controlled and monitored to ensure that the Company’s information is not compromised.

**13.0 SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**

**13.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS**

Security control requirements of the Company’s Information Systems shall be analyzed and specified. These requirements shall include, but are not limited to, web applications and transactions.

**13.2 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES**

Secure software and systems development shall be implemented. Changes to systems shall be controlled. Software packages shall ideally not be modified, and secure system engineering principles shall be followed. Application coding and development environment shall be secured, and outsourced development shall follow approved IT Security Controls. System security shall be tested and acceptance criteria defined to include security aspects. *(Refer to Software Development Policy for the details)*

**13.3 USING LIVE TEST DATA**

The use of live data for testing of new systems or system changes may only be permitted where adequate controls for the security of the data are in place.


**14.0 SUPPLIER MANAGEMENT** *(Refer to Third Party Partner Management Standards)*

**14.1 INFORMATION SECURITY IN SUPPLIER RELATIONSHIPS**

Protection of Company information that is accessible to IT outsourcers and other external suppliers throughout the supply chain shall be enforced. These protection procedures shall be agreed by all parties involved and stipulated in the contracts.

**14.2 SUPPLIER SERVICE DELIVERY MANAGEMENT**



	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

Service delivery by external suppliers shall be monitored, reviewed and audited against the contracts and agreements. Any change in services shall be controlled.

**15.0 INFORMATION SECURITY INCIDENT MANAGEMENT**

**15.1 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS**

All Information Security Incidents detected by or reported to IT shall be recorded, assessed, and resolved consistently and effectively in order to minimize the impact of such incidents to the Company. Forensic evidences shall be collected and protected. *(Refer to Standards on Detecting and Responding to Information Security Incidents for the details. – WIP\*)*

**16.0 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY** *(Refer to Standards on Planning for Business Continuity for the details. – WIP\*<sup>1</sup>)*

**16.1 INFORMATION SECURITY CONTINUITY**

The continuity of information security shall be planned, implemented and reviewed as an integral part of the Company’s business continuity management systems.

**16.2 FACILITIES REDUNDANCIES**

IT facilities shall have sufficient redundancy to satisfy availability requirements.

**17.0 COMPLIANCE**

**17.1 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS**

Appropriate procedures shall be implemented to ensure compliance with legal and contractual requirements.


**17.2 INFORMATION SECURITY REVIEWS**

Information security shall be implemented and operated in accordance with the organizational policies and procedures.

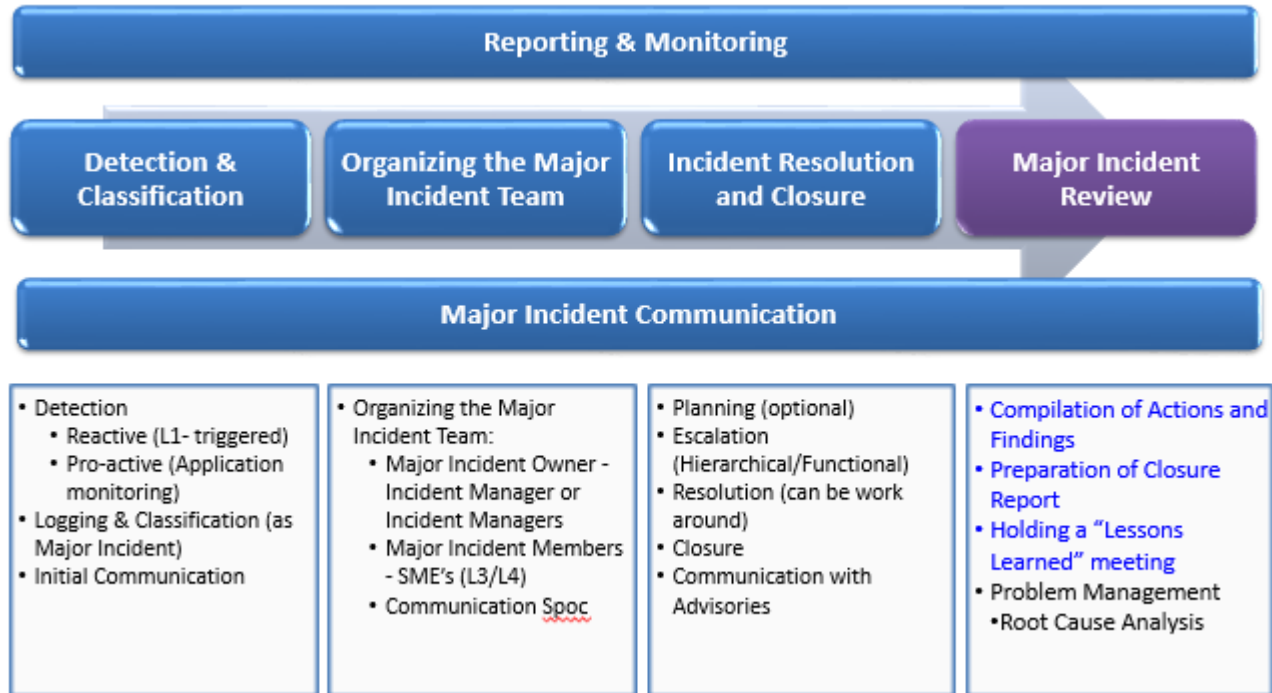
**END OF DOCUMENT**  
**General Information Security**  
**Policy**

---

<sup>1</sup> WIP: Work in Progress

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017


### Information Security Incident Process



*\*Information security incidents would follow the general flow of Incident Management Process*

### Some Types of Information Security Threats

Threat	Description
Unauthorized Access	Unauthorized successful logical access to an ABS-CBN IT resource or unauthorized access to customer IT resource from ABS-CBN Infrastructure
Denial of Service (DoS)	An attack that successfully prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the DoS.
Malicious Code	Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. IT GROUP team is NOT required to report malicious alerts that have been successfully quarantined by antivirus (AV) Software.
Data Leakage	Security incident involving loss of business information that has negative impact on ABS-CBN and/ or its Clients.

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

Improper Usage	Actions involving IT assets that violate Acceptable Use Policy. <u>Examples:</u> <ul style="list-style-type: none"> <li>• Downloading unauthorized security tools</li> <li>• Using ABS-CBN IT resource for non-business purpose</li> <li>• Using P2P activities to acquire or distribute pirated material</li> </ul>
----------------	--

### Information Security Incident Roles

Role	InfoSec Incidents
CORE	
Incident Lead/ Owner	Head of InfoSec
Incident Manager	InfoSec Analyst
L1 Support	Service Desk Analyst
L2 Support	-
L3 Support	SME
L4 Support (depending on the case)	Cyber Investigator, Forensic Investigator
SUPPORT	
Support Functions	IT HR-ER/LR Legal Services Compliance Corporate Communications Risk Management Physical Security

### Additional Incident Management Process Roles (Information Security Related)

Role	Responsibility
L3 Support (Cyber Investigator) = InfoSec Analyst	Specialized cyber technicians who shall be responsible for investigating a number of cases that range from suspected malware infections, unknown suspicious activities in the systems, and also be responsible for new technology review, investigations operating procedure enhancements and knowledge dissemination. Their responsibilities include: <ul style="list-style-type: none"> <li>• Handle investigation cases that are escalated by Incident Handlers</li> <li>• Liaise with legal teams as expert witness</li> <li>• Identify and recommend methods for efficient incident handling</li> <li>• Provide security knowledge training to Information Security teams and other relevant teams as necessary</li> </ul>



**INFORMATION SECURITY**


Information Technology Division

**Information Security Policies**

Prepared By Information Technology

Policy Owner Information Technology Last Update By/ Date May 19, 2017

<b>Role</b>	<b>Responsibility</b>
L3 Support (Forensic Investigator) = InfoSec Analyst	Expert digital forensic investigator who shall handle cases that require forensic analysis of digital evidences.
<b>IT</b>	IT custodians responsible for the upkeep of ABS-CBN IT infrastructure <ul style="list-style-type: none"> <li>• Perform regular backup of systems, maintain previous backup for specified time</li> <li>• Enable auditing on workstations, servers, and network devices</li> <li>• Assist ISIRT with necessary support during the course of investigation</li> <li>• Report suspected abnormal activities to Service Desk and Information Security</li> </ul> Provide standby IT assets for testing and investigation purposes
<b>HR- ER/LR</b>	<ul style="list-style-type: none"> <li>• Request and/or assist with Information Security investigations involving ABS-CBN employees.</li> <li>• Determine the motives of the act and recommend necessary action based on the Company Code of Conduct (COC)</li> <li>• Request technical help from Information Security for official data removal from the personal devices like memory drive, laptops etc.</li> <li>• Request technical help from Information Security in reviewing the personal mails of the employees</li> </ul> Update the ISIRT about the disciplinary actions taken
<b>Legal Services</b>	<ul style="list-style-type: none"> <li>• Provide advice and guidance regarding legal issues arising from incidents and investigations</li> </ul> Facilitate interactions with law enforcement agencies requesting information
<b>Compliance</b>	Ensure that the Company meets statutory, regulatory and contractual obligations triggered by an Information Security incident
<b>Corporate Communications</b>	<ul style="list-style-type: none"> <li>• Handle all media and investor relations in collaboration with Information Security</li> </ul> Ensure all publicized security incidents are handled in accordance with ABS-CBN's strategic message
<b>Risk Management</b>	Provide risk requirements and areas of concern
<b>Physical Security</b>	Ensure that the physical location of affected IT Resources and other critical areas are secured during incident response.

	<b>INFORMATION SECURITY</b>		
	Information Technology Division		
	<b>Information Security Policies</b>		
	Prepared By	Information Technology	
Policy Owner	Information Technology	Last Update By/ Date	May 19, 2017

### Severity for Information Security–Related Incidents

FACTORS	SEVERITY LEVEL	
	SEVERITY-1 CRITICAL	SEVERITY-2 HIGH
Data Classification	Incident involves compromised / changed data that involves personal information or is confidential in nature (e.g. personal sensitive information)	No data was stolen, changed or compromised OR Incident involves compromised / changed data for general company use
People	Incident affects multiple internal users from multiple business groups / networks or the entire Company OR Incident affects one or more company executive and/or executive staff OR Incident affects more than one customer	Incident affects one or a few internal users or a business group, or network OR Incident affects a customer (isolated case)
Financial & Reputation	Incident involves significant loss of company income (more than 1,000,000 PHP), faces media coverage	Incident involves minor loss of company income (less than 1,000,000PHP)
Business Operations	Incident impacts major disruption of business. The company is unable to provide critical services to a group or to all of its users / customers.	Incident impacts minor disruption on business. The company is able to provide their services but with less efficiency. (e.g, makes use of workaround procedures to deliver service)