


Information Security Measurement Guidelines

Ncell

Guidelines

Approved Date:- 13/12/2019

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO


Guideline Name DOCID: GD-IT-IS-12

Copyright © Ncell. All rights reserved.

No part of this document may be reproduced or transferred in any form or by any means without prior permission in writing from Ncell.

These trademarks are the intellectual property of Ncell and are protected by applicable legislation.

All other products or company names are used for reference only and may be proprietary to their respective hold

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Document Control

i. Document Identification

Document Title and Version:	GD-IT-IS-12 Information Security Measurement Guidelines v1.0
Effective Date:	5 th October, 2019
Document Author:	Information Security Team
Owner:	Information Security Team
Approved By:	CEO

ii. Distribution List

All Ncell Employees
Relevant External Parties and Auditor's (If Required)


iii. Document Roles and Responsibilities

Responsible	Information Security Team
Accountable	CIO/Head of IT
Consulted	Information Security Team and Function Heads
Informed	All Employees and Relevant External Parties

iv. Digital Signature

CEO

CIO/Head Of IT

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

v. Revision History

Rev	Date	Author	Description	Approved By	Initiated Date
0	05-10-2019	Information Security Team	Initial document	Vishal Mani Upadhyay	13-12-2019
1	13-12-2019	Tarani Prasad Chaudhary	Revised-Formatting/ Approval	Andy Chong	13-12-2019
2	20-08-2021	Information Security Team	Reviewed with no change	Vishal Mani Upadhyay	19-12-2021
3	19-12-2021	Tarani Prasad Chaudhary	Review-Formatting	Andy Chong	20-12-2019
4	25-08-2023	Information Security Team	2. Review changed from annual to once every two years. Added Head of IT	Rajesh Lal Nyachhyon	27-12-2023
5	27-12-2023	Tarani Prasad Chaudhary	Minor Formatting Approval	Rajesh Lal Nyachhyon Jabbor Kayumov	27-12-2023
6	25-04-2024	Information Security Team	Re-branding	CIO/Head of IT	



	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Table of Contents

Document Control	2
1. Purpose	5
2. Review and Updating	5
3. Scope	5
4. Classification	5
4.1 Implementation Measures	5
4.2 Impact Measures	5
4.3 Measurements to be reported	5
i. Measure 1: Security Budget (program-level)	5
ii. Measure 2: Vulnerability Management (program-level)	6
iii. Measure 3: Awareness and Training (AT) (program-level)	7
iv. Measure 4: Identification and Authentication (IA) (system-level)	8
v. Measure 5: Incident Response (program-level and system-level) (IR)	9
vi. Measure 6: Media Protection (MP) (program-level and system-level)	10
vii. Measure 7: Risk Assessment (RA) (system-level)	11
viii. Measure 8: System and Information Integrity (SI) (program-level and system-level)	12
5. Governance and Compliance	14
6. Associated Documents	14

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

1. Purpose

Ncell shall ensure all maintenance, diagnostic, and repair activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location, are managed and monitored to preserve the confidentiality, integrity, and availability of Ncell's information systems.

2. Review and Updating

This procedure shall be reviewed annually or whenever significant changes occur in the organization.

3. Scope

This guideline shall be applicable to all employees of Ncell; as well as Third party vendors, contractors, partners, collaborators and any others doing business or research with Ncell will be subject to the provisions of this standard. Any other parties, who use, work on, or provide services involving Ncell's computers, technology systems, and/or data will also be subject to the provisions of this guideline.

4. Classification

4.1 Implementation Measures

Implementation measures are used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures. Examples of implementation measures related to information security programs include the percentage of information systems with approved system security plans and the percentage of information systems with password policies configured as required.

4.2 Impact Measures


- Depending upon the organization's mission, impact measures can be used to quantify:
- Cost savings produced by the information security program or through costs incurred from addressing information security events;
- The degree of public trust gained/maintained by the information security program; or
- Other mission-related impacts of information security.

4.3 Measurements to be reported

The following are the measurements which have to be reported. The control families mentioned in the measure are referenced from NIST SP 800-53.

i. Measure 1: Security Budget (program-level)

Field	Data
Measure ID	Security Budget Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security Goal:</i> Provide resources necessary to properly secure agency information and information systems.
Measure	Percentage (%) of the agency's information system budget devoted to information security NIST SP 800-53 Controls – SA-2; Allocation of Resources
Measure Type	Impact
Formula	(Information security budget/total agency information technology budget) *100
Target	<To be defined by the Group CISO>.


	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Implementation Evidence	1. What is the total information security budget across all agency systems (SA-2)? _____ 2. What is the total information technology budget across all agency systems (SA-2)? _____
Frequency	Collection Frequency: Annually Reporting Frequency: Annually
Responsible Parties	<ul style="list-style-type: none"> Information Owner: Chief Information Officer (CIO), Chief Financial Officer (CFO) Information Collector & Reporter: Information Security Team Information Customer: Chief Information Officer (CIO)
Data Source	Exhibit 300s, Exhibit 53s, agency budget documentation

ii. Measure 2: Vulnerability Management (program-level)

Field	Data
Measure ID	Vulnerability Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security Goal:</i> Ensure all vulnerabilities are identified and mitigated.
Measure	Percentage (%) of high ¹ vulnerabilities mitigated within organizationally defined time periods after discovery NIST SP 800-53 Controls: RA-5; Vulnerability Scanning
Measure Type	Effectiveness/ Efficiency
Formula	(Number of high vulnerabilities identified and mitigated within targeted time frame during the time period /number of high vulnerabilities identified within the time period) *100
Target	90%
Implementation Evidence	1. Number of high vulnerabilities identified across the enterprise during the time (RA-5)? _____ 2. Number of high vulnerabilities mitigated across the enterprise during the time (RA-5)? _____
Frequency	Collection Frequency: Quarterly Reporting Frequency: Quarterly


¹ The National Vulnerability Database (NVD) provides severity rankings of "Low" "Medium" and "High" for all Common Vulnerabilities and Exposures (CVE) in the database. The NVD is accessible at <http://nvd.nist.gov>.

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Responsible Parties	<ul style="list-style-type: none"> Information Owner: Chief Information Officer (CIO), System Owner Information Collector & Reporter: Information Security Team Information Customer: Chief Information Officer (CIO)
Data Source	Vulnerability scanning software, audit logs, vulnerability management systems, patch management systems, change management records
Reporting Format	Stacked bar chart illustrating the percentage of high vulnerabilities closed within targeted time frames after discovery over several reporting periods

iii. Measure 3: Awareness and Training (AT) (program-level)


Field	Data
Measure ID	Security Training Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Ensure a high-quality work force supported by modern and secure infrastructure and operational capabilities. <i>Information Security Goal:</i> Ensure that organization personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.
Measure	Percentage (%) of information system security personnel that have received security training NIST SP 800-53 Controls: AT-3: Security Training
Measure Type	Implementation
Formula	(Number of information system security personnel that have completed security training within the past year/total number of information system security personnel) *100
Target	90%

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Implementation Evidence	<p>1. Are significant security responsibilities defined with qualifications criteria and documented in policy (AT-1 and PS-2)?</p> <p>Yes No</p> <p>2. Are records kept of which employees have significant security responsibilities (AT-3)?</p> <p>Yes No</p> <p>3. How many employees in your agency (or agency component, as applicable) have significant security responsibilities (AT-3)? _____</p> <p>4. Are training records maintained (AT-4)? (Training records indicate the training that specific employees have received.)</p> <p>Yes No</p> <p>5. How many of those with significant security responsibilities have received the required training (AT-4)? _____</p> <p>6. If all personnel have not received training, state all reasons that apply (AT-4):</p> <p>Insufficient funding Insufficient time Courses unavailable Employee has not registered Other (specify) _____</p>
Frequency	Collection Frequency: Quarterly Reporting Frequency: Quarterly
Responsible	• Information Owner: Information Security Team
Parties	• Information Collector and Reporter: Information Security Team • Information Customer: Chief Information Officer (CIO)
Data Source	Training and awareness tracking records
Reporting Format	Pie chart illustrating the percentage of security personnel that have received training versus those who have not received training. If performance is below target, pie chart illustrating causes of performance falling short of targets

iv. Measure 4: Identification and Authentication (IA) (system-level)


Field	Data
Measure ID	User Accounts Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security Goal:</i> All system users are identified and authenticated in accordance with information security policy.

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Measure	Percentage (%) of users with access to shared accounts NIST SP 800-53 Controls – AC-2: Account Management, AC-3: Access Enforcement, and IA-2: User Identification and Authentication
Measure Type	Effectiveness/Efficiency
Formula	(Number of users with access to shared accounts/total number of users) *100
Target	20%
Implementation Evidence	1. How many users have access to the system (IA-2)? _____ 2. How many users have access to shared accounts (AC-2)? _____
Frequency	Collection Frequency: Monthly Reporting Frequency: Monthly
Responsible Parties	<ul style="list-style-type: none"> Information Owner: System Owner, System Administrator Information Collector & Reporter: System Administrator, System Owner Information Customer: Chief Information Officer (CIO)
Data Source	Configuration Management Database, Access Control List, System-Produced User ID Lists
Reporting Format	Pie chart comparing the percentage of users with access to shared accounts versus the percentage of users without access to shared accounts

v. Measure 5: Incident Response (program-level and system-level) (IR)


Field	Data
Measure ID	Incident Response Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Make accurate, timely information on the organization's programs and services readily available. <i>Information Security Goal:</i> Track, document, and report incidents to appropriate organizational officials and/or authorities.
Measure	Percentage (%) of incidents reported within required time frame per applicable incident category (the measure will be computed for each incident category described in Implementation Evidence) NIST SP 800-53 Controls – IR-6: Incident Reporting
Measure Type	Effectiveness/Efficiency
Formula	For each incident category (number of incidents reported on time/total number of reported incidents) *100
Target	98 %

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Implementation Evidence	<p>1. How many incidents were reported during the period (IR-6)? Category 1 – Unauthorized Access? _____ Category 2 – Denial of Service? _____ Category 3 – Malicious Code? _____ Category 4 – Improper Usage? _____ Category 5 – Scans/Probes/Attempted Access? _____ Category 6 – Investigation? _____</p> <p>2. How many incidents involving personally identifiable information (PII) were reported during the period (IR-6)? _____</p> <p>3. Of the incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT (IR-6)? Category 1 – Unauthorized Access? _____ Category 2 – Denial of Service? _____ Category 3 – Malicious Code? _____ Category 4 – Improper Usage? _____ Category 5 – Scans/Probes/Attempted Access? _____ Category 6 – Investigation? _____</p> <p>4. Of the PII incidents reported, how many were reported within the prescribed time frame for their category, according to the time frames established by US-CERT and/or OMB Memorandum(s) (IR-6)? _____</p>
Frequency	Collection Frequency: Monthly Reporting Frequency: Annually
Responsible Parties	<ul style="list-style-type: none"> Information Owner: Incident Response Team (IRT) Information Collector & Reporter: Information Security Team Information Customer: Chief Information Officer (CIO)
Data Source	Incident logs, incident tracking database (if available)
Reporting Format	For one-time snapshot – stacked bar chart illustrating the proportion of reported incidents per category that were reported on time For trends – line chart where each line represents an individual category plus a line representing 100 percent

vi. Measure 6: Media Protection (MP) (program-level and system-level)


Field	Data
Measure ID	Media Sanitization Measure 1
Goal	<ul style="list-style-type: none"> <i>Strategic Goal:</i> Ensure an environment of comprehensive security and accountability for personnel, facilities, and products. <i>Information Security Goal:</i> Sanitize or destroy information system media before disposal or release for reuse.

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Measure	Percentage (%) of vulnerabilities remediated within organization-specified time frames NIST SP 800-53 Controls – RA-5: Vulnerability Scanning and CA-5: Plan of Actions and Milestones
Measure Type	Effectiveness/ Efficiency
Formula	(Number of vulnerabilities remediated according to POA&M schedule/total number of POA&M documented vulnerabilities identified through vulnerability scans) *100
Target	90%
Implementation Evidence	<p>1. Does the organization conduct periodic vulnerability scans (RA-5)?</p> <p>Yes No</p> <p>2. What is the periodicity of vulnerability scans (RA-5)?</p> <p>Weekly</p> <p>Monthly</p> <p>Quarterly</p> <p>Other _____</p> <p>3. Does the organization's POA&M process require vulnerabilities identified through vulnerability scanning to be documented in appropriate system POA&Ms (CA-5)?</p> <p>Yes No</p> <p>4. How many vulnerabilities were identified through vulnerability scanning and entered into applicable POA&Ms (CA-5)? _____</p> <p>5. How many of the vulnerabilities from Question 4 were remediated on schedule according to their POA&Ms (CA-5)? _____</p>
Frequency	Collection Frequency: Monthly Reporting Frequency: Monthly
Responsible Parties	<ul style="list-style-type: none"> Information Owner: System Owners Information Collector & Reporter: Information Security Team Information Customer: Chief Information Officer (CIO)
Data Source	POA&Ms, vulnerability scanning reports
Reporting Format	Pie chart comparing the percentage of vulnerabilities remediated on schedule versus the e percentage of vulnerabilities not remediated on schedule

viii. Measure 8: System and Information Integrity (SI) (program-level and system-level)

Field	Data
-------	------

	Ncell	Classification: Internal
	Information Security Measurement Guidelines	Owner: CIO/Head of IT
		Effective Date: 5 th Oct, 2019
Prepared by: Information Security Team	Controlled by: Business Continuity & Process Management	Approved by MD/CEO

Reporting Format	Stacked bar chart with total number of applicable vulnerabilities composed of percentages of number of vulnerabilities addressed in distributed alerts and advisories for which patches have been determined as non-applicable, have been implemented, have had a waiver granted, or other
------------------	--

5. Governance and Compliance

- i. There shall be no exceptions to these guidelines.
- ii. Internal and external compliance review shall be conducted as per the organization internal and external audit requirements.

6. Associated Documents

- i. Information Security Policy