

PATCH MANAGEMENT POLICY



COGENT E SERVICES PRIVATE LTD.

C 100, Sector 63,
Noida GautamBudh Nagar
Uttar Pradesh 201301,
INDIA .

www.cogenteservices.com

To protect the confidential and proprietary information included in this material, it may not be disclosed or provided to any third parties without the approval of Cogent E Services Management.

Table of Contents

TABLE OF CONTENTS	2
SECTION-I DOCUMENT DETAILS.....	4
DOCUMENT INFORMATION	4
VERSION CONTROL PROCEDURE	4
VERSION HISTORY	5
DISTRIBUTION AND CONTROL	5
SECTION-II ISMS PATCH MANAGEMENT POLICY	6
1. Purpose	6
2. Scope.....	6
3. Definitions	7
4. Policy	7
5. Violation of Policy.....	9
6. Enforcement.....	10
SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES	11
STAKEHOLDER	11
RACI MATRIX	14
SECTION 5 – POLICY GOVERNANCE	16
AUDITING.....	16
POLICY CLARIFICATION.....	16
POLICY VIOLATIONS	16
COMPLIANCE	16
EXCEPTIONS	16
REVIEW.....	17
REPORTING	17
DISTRIBUTION OF POLICY	17
SECTION 6 – DEFINITIONS	18
SECTION 7 – APPENDIX.....	19
APPLICABLE FORMATS	19

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 2 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 3 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

SECTION-I DOCUMENT DETAILS

DOCUMENT INFORMATION

Preface

The Cogent E Services Information Security Management System (ISMS) Team assumes responsibility for this document and updates it as required to meet the needs of users. The Cogent E Services ISMS Team welcomes and solicits feedback from users of this document and its reference artifacts so that future revisions of this document will reflect improvements, based on new technology, organizational best practices, and lessons learned.

Copyright

This document contains proprietary information for Cogent E Services. It may not be copied, transferred, shared in any form by any agency or personnel except for authorized internal distribution by Cogent E Services, unless expressly authorized by Cogent E Services Information Security Steering Committee in writing.

VERSION CONTROL PROCEDURE

Draft Version: Any version of this document before it is finalized by all stakeholders i.e., process owners, client and ISO internal auditors, would be treated as 'Draft Version'.

The control number for the draft version would always start from '0'. For example first draft will have the control number as 0.1.

Final Version: Once the document is finalized by all stakeholders i.e., process owners, client and ISO Internal Auditor, it will cease to be a 'draft' and will be treated as 'final version'.

To distinguish between draft version and final version, the control number for finalized document would always start from an integer, greater than zero. For example, first final version will have the control number as 1.0.

Document Creation and Maintenance: This document would generally be written for the first time at the time of transition to ISO/IEC 27001:2013. It will be maintained by the Information Security Manager (ISM) and is subjected to review at a minimum on a yearly basis. The Information Security Steering Committee (ISF) members are responsible for approving any necessary amendments to the Cogent E Services Information Security Policy Documents. Changes to the Cogent E Services, ISMS Policy and ISMS Objectives shall be reviewed by the CISO and approved by Cogent E Services Information Security Steering Committee.

Implementation Date: Implementation date is the date when the document is released and made operational in the ISMS. By logic, it should be after the approval date. All dates should be updated in MM/DD/YYYY format.

Amendment Procedure: The Cogent E Services Information Security Policy Documents shall be amended to reflect any changes to Cogent E Services capability or the Information Security Management System.

Summary of Changes: Version history table below denotes the nature and context of any update or change made in this document.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 4 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

VERSION HISTORY

Version	Prepared by		Reviewed by		Approved by		Implementation Date	Summary of Changes
	By	Date	By	Date	By	Date		
0.1	ISM	03rd Dec'14	CISO	05th Dec'14	ISSC	-----	-----	Initial Draft
1	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	First Revision
1.0	ISM	30th Dec'14	CISO	30th Dec'14	ISSC	30th Dec'14	1st Jan'15	New Template and updated document
1.1	ISM	13th Nov'15	CISO	13th Nov'15	ISSC	13th Nov'15	2nd Jan'16	
1.2	ISM	15th Oct'16	CISO	15th Oct'16	ISSC	15th Oct'16	31st Dec'16	
2.0	ISM	15th dec'17	CISO	15th dec'17	ISSC	15th dec'17	1st Jan'18	
2.1	ISM	22nd dec'18	CISO	22nd dec'18	ISSC	22nd dec'18	3rd Jan'19	
3.0	ISM	07 th Dec'19	CISO	07 th Dec'19	ISSC	07 th Dec'19	10th Dec'19	
3.1	ISM	07 Jul'21	CISO	07 Jul'21	ISSC	07 Jul'21	11th Jul'21	
3.2	ISM	07 Apr'22	CISO	07 Apr'22	ISSC	07 Apr'22	11th Apr'22	

DISTRIBUTION AND CONTROL
Document Distribution

The Cogent E Services Chief Information Security Officer (CISO) shall distribute this document to all document change reviewer when it is first created and as changes or updates are made. The CISO shall distribute the document to members of Information Security Steering Committee (hereinafter referred to as ISSC) and Information Security Working Group (hereinafter referred to as ISWG).

The softcopy of the manual and related documents will be accessible to all employees in read-only mode through intranet

One set of hard copies will be available with the CISO as controlled copy. All other soft and hard copies of the ISMS documents are deemed to be uncontrolled. The CISO will ensure that any

Prepared by: INFORMATION SECURITY MANAGER	Approved by: INFORMATION SECURITY STEERING COMMITTEE	Issued by: CHIEF INFORMATION SECURITY OFFICER	Page no. Page 5 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

update to the ISMS is incorporated on the intranet server and is communicated to all employees of Cogent E Services through an appropriate mode such as e-mail.

Distribution List

Name	Title
Information Security Steering Committee	ISSC
Information Security Working Group	ISWG
Chief Information Security Officer	CISO

Conventions

The statements containing the words 'shall' and 'required to' in the document are mandatory rules. Failure to observe these rules may be construed as non-compliance to the policy.

The statements containing the words 'should' and 'recommended' imply a desirable requirement. Failure to adhere to these rules may not be a direct non-compliance.

SECTION-II ISMS PATCH MANAGEMENT POLICY

1.Purpose

The purpose of this policy is to ensure computer systems attached to the Cogent E Services network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

2.Scope

This policy applies to all employees of Cogent E Services.; as well as vendors, contractors, partners, collaborators and any others doing business or research with the Cogent E Services will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving Cogent E Services computers, technology systems, and/or data will also be subject to the provisions of this policy.

Cogent E Services computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the educational, clinical, and research missions of the school. This policy will not supersede any Cogent E Services Global developed policies but may introduce more stringent requirements than the university policy.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 6 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

3. Definitions

Operating System (OS) is the set of programs used to provide the basic functions of a computer.

A device is defined as any object used to store, process, and/or transfer data.

Confidentiality, Integrity, Availability (CIA) is the three basic tenets of information security.

A networked device is defined as any device that is either permanently or periodically attached to the Cogent E Services network.

Remediate is defined as all patches required by the vendor have been applied.

Mitigated is defined as steps have been taken to protect a device from a particular vulnerability, i.e. the device has been removed or otherwise isolated from the network, the NIC card has been removed, or an approved deviation from the required patch process has been approved by the Cogent E Services Chief Security Officer (CSO) and is on file.

4. Policy

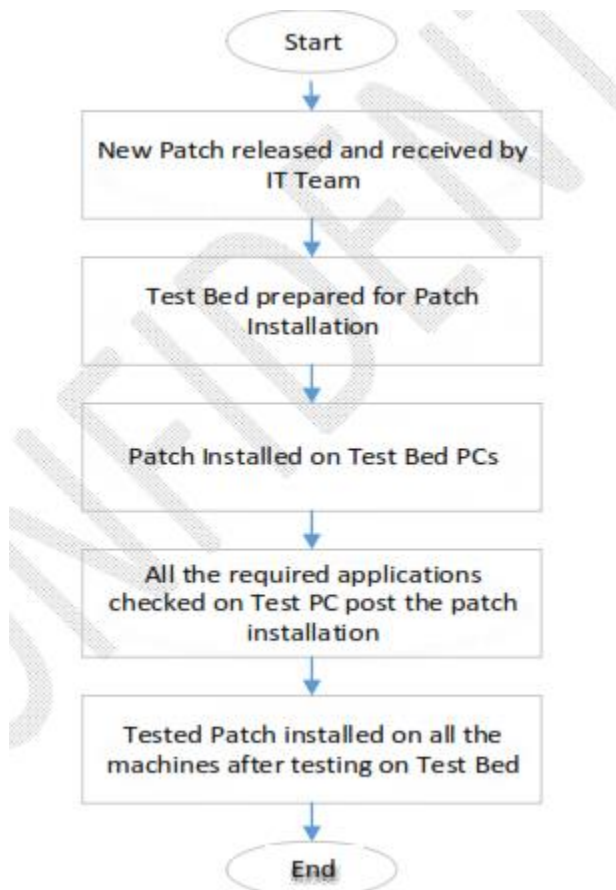
1. All networked devices belonging to or managed by Cogent E Services Global departments, practice plans, or other affiliated and partner organizations will be patched with vendor provided operating system security patches.
2. These patches will be applied as soon as possible following appropriate testing of the security patches by the Cogent E Services departments, practice plans, or other affiliated and partner organizations.
3. New devices must be patched to the current patch level, as defined by the operating system vendor, PRIOR to the device being connected to the production network.
4. Current patch status for all Cogent E Services departments, practice plans, or other affiliated and partner organizations must be communicated to the Cogent E Services ISO or designate. Devices that cannot be patched will report the exact mitigation effort to the ISO or designate.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 7 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 8 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

5. Patch Management Process

1. New Patch received by IT team.
2. Test bed prepared for Patch installation.
3. Patch installed and tested on testing PC (Test Bed)
4. All required applications tested on the test PC post patch installation.
5. All the machines updated with the patch after successful testing on test bed PCs.



6. Violation of Policy

If it is suspected that this policy is not being followed, report the incident to the Departmental IT manager or representative and the Cogent E Services Security Officer.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 9 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

Any exceptions to this policy must be approved in advance by both the Cogent E Services Security Officer and the Chief Information Officer.

7.Enforcement

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Cogent E Services Policy.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 10 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

SECTION 3 – STAKEHOLDER - ROLES AND RESPONSIBILITIES

STAKEHOLDER

Stakeholder	Roles & Responsibility
Managing Director	<ul style="list-style-type: none"> Providing Overall Direction and leadership to Organization Ensuring that adequate resources and provisions are in place for the continued protection of Information assets of Cogent E Services.
Director Operations	<ul style="list-style-type: none"> Ensuring quality and security issues that may affect the Cogent E Services Business and Strategic Plans are considered. Authorize and decide on new security products to be implemented across Cogent E Services
Director Corporate Affairs	<ul style="list-style-type: none"> Ensuring continued compliance with Cogent E Services business objectives and external requirements
Information Security Steering Committee	<ul style="list-style-type: none"> The committee shall take overall responsibility for Quality and Information security, including Ratification of the Quality Management and Information Security Policies and Procedures suggested by the CISO. Ensure that Quality and Information Security Policies and Procedures can be implemented by ensuring the involvement of the appropriate business heads. Initiating internal and external security reviews and ensuring that action is taken to rectify any shortfalls identified.
Chief Information Security Officer	<ul style="list-style-type: none"> CISO is responsible for effectively conducting management review meetings & provides guidance for improvements. CISO is responsible for Organizing management review meetings, Reporting on performance of ISMS and ISMS at Cogent E Services Maintaining records of Management Review meetings & Take follow up actions

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 11 of 19

Stakeholder	Roles & Responsibility
	<ul style="list-style-type: none"> Establishes and maintains process and product audit schedule. Monitors and controls the day-to-day QA activities and schedule. Escalates unresolved non-compliance issues to the ISM Committee Identifies training required to perform the tasks which includes training of the QA Group and QA orientation for the project team members.
Information Security Manager	<ul style="list-style-type: none"> Provide direction and support for security implementation Support the risk management process by analyzing threats to the computing environment. Analyze reports submitted and the work performed by ISO 27001 Core Team and take corrective action. Ensure that ongoing information security awareness education and training is provided to all Cogent E Services employees during security project implementation In co-ordination with Internal Audit guidelines, incorporate appropriate procedures in the routine audit checks to verify the compliance to the Cogent E Services Information Security Policy and detect incidents.
Internal Auditor/s	<ul style="list-style-type: none"> Identify areas/processes where audits are required Prepare audit plan; Select audit team member; Prepare audit report; Report audit conclusion to Information Security Steering Committee .Performs the audit using the consolidated audit checklist. Reports the non-conformities and recommends suggestions for improvement
Information Security Coordinator and Document Controller	<ul style="list-style-type: none"> Ensure Documents & records are stored and maintained in a central location & in proper manner for retrieval and backup

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 12 of 19

Stakeholder	Roles & Responsibility
	<ul style="list-style-type: none"> Assures all documents are properly formatted Handle records according to their classification Ensure records are maintained in a proper manner for retrieval;
Head of Department	<ul style="list-style-type: none"> Operations Representative will be responsible for preparing and maintaining Information Security Policies & Procedures within Operations at Cogent E Services. Create security awareness within Operations at Cogent E Services Provide a report of Cogent E Services Information Security Policy violations and IT security incidents as and when they occur, else a clean statement. Oversee all information security processes and serve as the focal point for all information security issues and concerns. To bring any possible security threats to the notice of Cogent E Services.
Employee /s	<ul style="list-style-type: none"> Adhere to Cogent E Services Policy and procedure Suggest remedial measures to non-conformities detected. Suggest document change for processes if required

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 13 of 19

RACI MATRIX

The following table identifies who within Cogent E Services is Accountable, Responsible, Informed or Consulted with regards to this documented policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	ISMS Lead Auditor
Accountable	Corporate Information Security Officer
Consulted	ISWG
Informed	ISSC

CISO/IS Manager in their role as Cogent E Services Chief Information Security Officer are /is responsible for effectively conducting management review Meetings & provides guidance for improvements. CISO is responsible for

- Organizing management review meetings,
- Reporting on performance of Cogent E Services ISMS
- Maintaining records of Management Review meetings &
- Take follow up actions
- Identify areas/processes where audits are required
- Designate person responsible for auditing the processes
- Ensure the effective implementation of audit procedure within their area of responsibility
- Prepare audit program
- Monitor the performance of the internal audit activities;
- Present the summary of audit findings at the Management Review Meeting;
- Maintain all internal audit records.
- Ensure that the audit of the process(s) is carried out periodically and without hindrance.
- Suggest remedial measures to non-conformities detected.
- Suggest document change for processes if required.
- Designate person responsible for as Information Security Manager/ Coordinator for CAPA in the various processes
- Ensure the effective implementation of CAPA procedure within their area of responsibility

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 14 of 19

SECTION 4 – PERFORMANCE MEASURES

CRITICAL SUCCESS FACTORS:

S. No.	Critical Success Factors
1	Top Management Support & Commitment
2	Effective & Timely Management Reviews
3	Adherence to Procedure by all concerned
4	Regular Management Reviews
5	Regular Reviews of Follow-up of Actions arising from Management Reviews & Internal Audits

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 15 of 19

SECTION 5 – POLICY GOVERNANCE

AUDITING

This policy will be audited at periodic intervals by the Cogent E Services Internal Audit team as per the Information Security Management System audit plan. Audit Findings will constitute one of the significant inputs for Management Reviews of this policy document.

POLICY CLARIFICATION

For general questions or clarification on any of the information contained in this policy, please contact Cogent E Services Chief Information Security Officer. For questions about department-wide Information Security policies and procedures contact the Cogent E Services Information Security Manager.

POLICY VIOLATIONS

Violations of this policy may include, but are not limited to any act that:

- Does not comply with the requirements of this policy;
- Results in loss of Cogent E Services information;
- Exposes Cogent E Services to actual or potential loss through the compromise of quality and or Information security;
- Involves the disclosure of confidential information or the unauthorized use of Cogent E Services information and information processing facilities;
- Involves the use of the hardware, software or information for unauthorized or illicit purposes which may include violation of any law, regulation or reporting requirements of any law enforcement or government body;
- Violates any laws which may be introduced by the Government from time to time in the region in which Cogent E Services is operating or providing services ;

COMPLIANCE

Violation of this policy may result in disciplinary action which may include suspension, termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of Cogent E Services Information Resources access privileges, other disciplinary actions including civil and criminal prosecution.

EXCEPTIONS

Deviations from this procedure can be exceptions or breaches. A deviation can either be permitted, or is then referred to as an exception, or not permitted, and is then referred to as a breach. Exceptions shall not be granted, unless exceptional conditions exist.

All requests for exceptions to this policy shall be addressed through the Cogent E Services Chief Information Security Officer

Requests for exceptions to policies must have a justifiable business case documented and must have the necessary approvals. Exceptions must be approved and signed by either:

- Managing Director, Cogent E Services Pvt. Ltd.
- Chief Information Security Officer

Once approved, exceptions to policy will be valid for a pre-decided period after which it must be re-evaluated and re-approved. All exceptions to policy must be communicated to Corporate Information Security Officer (CISO) or Information Security Manager (ISM) and captured in a Log by the Document controller.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 16 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

If policy exceptions are likely to circumvent existing internal controls then “Mitigating Controls” or “Compensating Controls” must be implemented and followed. The Cogent E Services ISMS Committee must be involved in all instances where Information Security controls are bypassed.

REVIEW

This policy must be reviewed once a year at a minimum or as the need arises along with all the stakeholders involved in this procedure and be re approved by Cogent E Services Information Security Steering Committee accordingly.

REPORTING

Any person who becomes aware of any Information Security issues, risks and or loss, compromise, or possible compromise of information, or any other incident which has Information Security implications, must immediately inform his/her immediate superior authority as the case may be, who shall initiate immediate action to prevent further compromise or loss.

DISTRIBUTION OF POLICY

The Policy is an internal document and is meant for internal usage within the company. Duplication and distribution of this policy without an authorized release is prohibited. The Cogent E Services ISMS Team will decide on the number of copies that will be in circulation and the persons with whom the document will be available.

Every person in custody of the document has the responsibility for ensuring its usage limited to “within the organization”. The custodian of the document will also ensure and that the document is continually updated with amendments that may be issued from time to time. Any loss or mutilation of the document must be reported promptly to the Cogent E Services Information Security Manager.

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 17 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			

SECTION 6 – DEFINITIONS

Word/Term	Definition
Information Security Management System (ISMS)	Management system to direct and control an organization with regard to Information Security.
Top Management	Person or group of people who direct and control an organization at the highest level.
Effectiveness	Extent to which planned activities are realized and planned results achieved.
Efficiency	Relationship between the results achieved and the resources used
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
Root Cause	Fundamental deficiency that results in a non-conformance and must be corrected to prevent recurrence of the same or similar non conformance
Continual Improvement	<p>recurring process which results in enhancement of Information Security performance and the Information Security management system</p> <p>NOTE 1 The process of establishing objectives and finding opportunities for improvement is a continual process.</p> <p>NOTE 2 Continual improvement achieves improvements in overall Information Security performance, consistent with the organization's Information Security policy.</p> <p><i>Is a process or productivity improvement tool intended to have a stable and consistent growth and improvement of all the segments of a process or processes? ... (Also called incremental improvement or staircase improvement). The process of establishing objectives and finding opportunities for improvement is a continual process through the use of audit findings and audit conclusions, analysis of data, management reviews or other means and generally leads to corrective action or preventive action.</i></p>

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 18 of 19

SECTION 7 – APPENDIX

APPLICABLE FORMATS

END OF DOCUMENT

Prepared by:	Approved by:	Issued by:	Page no.
INFORMATION SECURITY MANAGER	INFORMATION SECURITY STEERING COMMITTEE	CHIEF INFORMATION SECURITY OFFICER	Page 19 of 19
This document is for CESPL internal use. Full or no part of this document is to be reproduced in any mode or not to be taken out without permission of management.			