Central Procurement Technical Unit (CPTU)
Implementation Monitoring and Evaluation Division (IMED)
Ministry of Planning
Government of the People’s Republic of Bangladesh

Information Security Policy

For

Electronic Government Procurement (e-GP) System

November, 2019
**Document Control**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Type of Information</th>
<th>Document Data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Document Title</td>
<td>Information Security Policy</td>
</tr>
<tr>
<td></td>
<td>Document Code</td>
<td>CPTU/e-GP IS Policy/2019</td>
</tr>
<tr>
<td></td>
<td>Date of Release</td>
<td>November, 2019</td>
</tr>
<tr>
<td></td>
<td>Document Superseded</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Document Revision Number</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Document Owner</td>
<td>Director General, CPTU</td>
</tr>
<tr>
<td></td>
<td>Document Author</td>
<td>CPTU, IMED, Ministry of Planning</td>
</tr>
</tbody>
</table>

**Document Approvers**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Approver</th>
<th>Designation</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>M A Mannan</td>
<td>Honorable Minister, Ministry of Planning</td>
<td>07-01-2020</td>
</tr>
</tbody>
</table>

**Document Change Approval**

<table>
<thead>
<tr>
<th>Version</th>
<th>Revision Date</th>
<th>Nature of Change</th>
<th>Date Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Electronic Government Procurement (e-GP)
Preamble

National e-Government Procurement (e-GP) portal (i.e. https://www.eprocure.gov.bd) of the Government of the People’s Republic of Bangladesh is developed, owned and being operated by the Central Procurement Technical Unit (CPTU), IME Division of Ministry of Planning. It is a visionary step of the Government towards implementing e-Governance to accomplish the Vision 2021: Digital Bangladesh. e-GP deals with many sensitive information which should be retained classified and secure. In order to protect such valuable data from unauthorized access and manipulation, it is a fundamental requirement to have a proper security policy and implementation mechanism in place. Hence, it is an initiative from CPTU to publish the e-GP Information Security Policy following the Information Security Policy Guideline issued by ICT Division on 6th April 2014 through gazette notification.

The objective of the policy is to ensure necessary measures, incorporate various preventive, reactive, detective and administrative controls to endorse the major security principles - Confidentiality, Integrity and Availability of e-GP system and promote e-GP system security culture in e-GP management. Moreover, the policy will ensure management direction and support to implement information security of the e-GP system as per ISO 27001:2013 standard and Government of Bangladesh Information Security Manual.

e-GP Information Security Policy is a live document which will be updated periodically or as necessary by the Information Security Steering Committee (ISSC) as the information security trends are rapidly evolving with time.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abbreviations</td>
<td>viii</td>
</tr>
<tr>
<td>Definition</td>
<td>x</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2. Objective</td>
<td>2</td>
</tr>
<tr>
<td>3. Applicability and Scope</td>
<td>3</td>
</tr>
<tr>
<td>4. Data and Information Asset</td>
<td>5</td>
</tr>
<tr>
<td>4.1. Definition</td>
<td>5</td>
</tr>
<tr>
<td>4.2. Forms of data and information</td>
<td>5</td>
</tr>
<tr>
<td>4.3. Asset Classification</td>
<td>5</td>
</tr>
<tr>
<td>4.4. Information Owner</td>
<td>7</td>
</tr>
<tr>
<td>4.5. Information Custodian</td>
<td>7</td>
</tr>
<tr>
<td>5. Leadership</td>
<td>8</td>
</tr>
<tr>
<td>5.1. Leadership and commitment</td>
<td>8</td>
</tr>
<tr>
<td>5.2. Policy</td>
<td>9</td>
</tr>
<tr>
<td>5.2.1. Purpose</td>
<td>9</td>
</tr>
<tr>
<td>5.2.2. Policy statement</td>
<td>9</td>
</tr>
<tr>
<td>5.2.3. Implementation</td>
<td>10</td>
</tr>
<tr>
<td>5.2.4. Document owner</td>
<td>10</td>
</tr>
<tr>
<td>5.2.5. Document convention</td>
<td>10</td>
</tr>
<tr>
<td>5.2.6. Document distribution</td>
<td>10</td>
</tr>
<tr>
<td>5.2.7. Violation of the policy</td>
<td>10</td>
</tr>
<tr>
<td>5.2.8. Waiver criteria</td>
<td>11</td>
</tr>
<tr>
<td>6. Planning</td>
<td>12</td>
</tr>
<tr>
<td>6.1. Actions to address risks and opportunities</td>
<td>12</td>
</tr>
<tr>
<td>6.1.1. General</td>
<td>12</td>
</tr>
<tr>
<td>6.1.2. Information security risk assessment</td>
<td>12</td>
</tr>
<tr>
<td>6.1.3. Information security risk treatment</td>
<td>13</td>
</tr>
<tr>
<td>6.1.4. Information security objectives and planning to achieve them</td>
<td>15</td>
</tr>
<tr>
<td>7.1. Management Direction for Information Security</td>
<td>16</td>
</tr>
<tr>
<td>7.1.1. Policies for information security</td>
<td>16</td>
</tr>
<tr>
<td>7.1.2. Review of policy for Information security</td>
<td>16</td>
</tr>
<tr>
<td>8. Information Security Organization</td>
<td>17</td>
</tr>
</tbody>
</table>
### 8.1 Internal Organization

| 8.1.1 Information Security Committee Roles and Responsibilities | 17 |
| 8.1.2 Segregation of Duties (SOD) | 18 |
| 8.1.3 Contact with Authorities | 18 |
| 8.1.4 Contact with Special Interest Groups | 19 |
| 8.1.5 Information security in project management | 19 |
| 8.1.6 Portable Devices and Telecommuting | 19 |
| 8.1.6.1 Portable device policy | 19 |
| 8.1.6.2 Telecommuting | 20 |

### 9. Human Resources

| 9.1 Prior to Employment | 21 |
| 9.1.1 Screening | 21 |
| 9.1.2 Terms and conditions of employment | 21 |
| 9.2 During Employment | 22 |
| 9.2.1 Management Responsibilities | 22 |
| 9.2.2 Information Security awareness, education & training | 22 |
| 9.2.3 Disciplinary process | 22 |
| 9.3 Termination and change of employment | 22 |
| 9.3.1 Termination or change of employment responsibilities | 22 |

### 10. Assets Management

| 10.1 Responsibility for Assets | 23 |
| 10.1.1 Inventory of Assets | 23 |
| 10.1.2 Ownership of Assets | 24 |
| 10.1.3 Acceptable use of Assets | 24 |
| 10.1.4 Return of Assets | 26 |
| 10.2 Information Classification | 26 |
| 10.2.1 Labeling of Information | 26 |
| 10.2.2 Handling of Assets | 26 |
| 10.3 Media Handling | 26 |
| 10.3.1 Management of removable media | 26 |
| 10.3.2 Disposal of media | 27 |
| 10.3.3 Physical media transfer | 28 |

### 11. Access Control

| 11.1 Business Requirement for access control | 29 |
| 11.1.1 Access Control Policy | 29 |
| 11.1.2 Access to Networks and Network Services | 29 |
11.2. User Access Control Management
   11.2.1. User Registration and De-registration
   11.2.2. User Access Provisioning
   11.2.3. Management of Privilege Access Rights
   11.2.4. Management of Secret Authentication Information of Users
   11.2.5. Review of User Access Rights
   11.2.6. Removal or Adjustment of Access Rights

11.3. User Responsibilities
   11.3.1. Use of Secret Authentication Information

11.4. System and Application Access Control
   11.4.1. Information Access Restriction
   11.4.2. Secure Log-on Procedure
   11.4.3. Password Management System
   11.4.4. Use of Privileged Utility Program
   11.4.5. Access Control to Program Source Code
   11.4.6. Secure Coding Practice
   11.4.7 Database access policy

12. Cryptography

12.1. Cryptographic Controls
   12.1.1. Policy on Use of Cryptographic Controls
   12.1.2. Key management

13. Physical and Environmental Security

13.1. Physical Security Perimeter
   13.1.1. Physical Entry Controls
   13.1.2. Securing the Facilities
   13.1.3. Visitor Management
   13.1.4. Protecting Against external and environmental threats
   13.1.5. Working in Secure Areas
   13.1.6. Delivery and Loading Areas

13.2. Equipment Security
   13.2.1. Equipment Siting & Protection
   13.2.2. Supporting Utilities
   13.2.3. Cabling Security
   13.2.4. Equipment Maintenance
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.1</td>
<td>Network Security Management</td>
<td>49</td>
</tr>
<tr>
<td>15.1.1</td>
<td>Network Control</td>
<td>49</td>
</tr>
<tr>
<td>15.1.2</td>
<td>Security of network services</td>
<td>50</td>
</tr>
<tr>
<td>15.1.3</td>
<td>Segregation in Networks</td>
<td>50</td>
</tr>
<tr>
<td>15.2</td>
<td>Information Transfer</td>
<td>50</td>
</tr>
<tr>
<td>15.2.1</td>
<td>Information transfer policy and Procedures</td>
<td>50</td>
</tr>
<tr>
<td>15.2.2</td>
<td>Agreement on Information transfer</td>
<td>50</td>
</tr>
<tr>
<td>15.2.3</td>
<td>Electronic Messaging</td>
<td>51</td>
</tr>
<tr>
<td>15.2.4</td>
<td>Confidentiality or non-disclosure agreements</td>
<td>52</td>
</tr>
<tr>
<td>16</td>
<td>System Acquisition, Development and Maintenance</td>
<td>53</td>
</tr>
<tr>
<td>16.1</td>
<td>Security Requirement of Information Systems</td>
<td>53</td>
</tr>
<tr>
<td>16.1.1</td>
<td>Information Security Requirement Analysis and Specification</td>
<td>53</td>
</tr>
<tr>
<td>16.1.2</td>
<td>Securing application services on public networks</td>
<td>53</td>
</tr>
<tr>
<td>16.1.3</td>
<td>Protecting application services transactions</td>
<td>53</td>
</tr>
<tr>
<td>16.2</td>
<td>Security in Development and Support Processes</td>
<td>54</td>
</tr>
<tr>
<td>16.2.1</td>
<td>Secure Development Policy</td>
<td>54</td>
</tr>
<tr>
<td>16.2.2</td>
<td>System Change Control Procedure</td>
<td>54</td>
</tr>
<tr>
<td>16.2.3</td>
<td>Technical review of applications after operating platform changes</td>
<td>54</td>
</tr>
<tr>
<td>16.2.4</td>
<td>Restrictions on changes to software packages</td>
<td>54</td>
</tr>
<tr>
<td>16.2.5</td>
<td>Secure system engineering principles</td>
<td>54</td>
</tr>
<tr>
<td>16.2.6</td>
<td>Secure development environment</td>
<td>55</td>
</tr>
<tr>
<td>16.2.7</td>
<td>Outsourced development</td>
<td>55</td>
</tr>
<tr>
<td>16.2.8</td>
<td>System security testing</td>
<td>55</td>
</tr>
<tr>
<td>16.2.9</td>
<td>System acceptance testing</td>
<td>55</td>
</tr>
<tr>
<td>16.3</td>
<td>Test Data</td>
<td>56</td>
</tr>
<tr>
<td>16.3.1</td>
<td>Protection of test data</td>
<td>56</td>
</tr>
<tr>
<td>17</td>
<td>Supplier Relationships</td>
<td>57</td>
</tr>
<tr>
<td>17.1</td>
<td>Information security in Supplier relationships</td>
<td>57</td>
</tr>
<tr>
<td>17.1.1</td>
<td>Information Security Policy for Supplier relationship</td>
<td>57</td>
</tr>
<tr>
<td>17.1.2</td>
<td>Addressing security within supplier agreements</td>
<td>57</td>
</tr>
<tr>
<td>17.1.3</td>
<td>Information and communication technology supply chain</td>
<td>58</td>
</tr>
<tr>
<td>17.2</td>
<td>Supplier Service Delivery management</td>
<td>58</td>
</tr>
<tr>
<td>17.2.1</td>
<td>Monitoring and review of supplier services</td>
<td>58</td>
</tr>
<tr>
<td>17.2.2</td>
<td>Managing changes to supplier services</td>
<td>58</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>18. Information Security Incident Management</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>18.1. Management of information security incidents and improvements</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>18.1.1. Responsibilities and Procedures</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>18.1.2. Reporting information security events</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>18.1.3. Reporting information security Weaknesses</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>18.1.4. Assessment of and decision on information security events</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>18.1.5. Response to information security incidents</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>18.1.6. Learning from Information Security Incidents</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>18.1.7. Collection of Evidence</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>19.1. Information Security Continuity</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>19.1.1. Planning Information Security Continuity</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>19.1.2. Implementing information security continuity</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>19.1.3. Verify, review and evaluate information security continuity</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>19.2. Redundancies</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>19.2.1. Availability of information processing facilities</td>
<td>63</td>
<td></td>
</tr>
<tr>
<td>20. Compliance Policy</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1. Compliance with Legal and Contractual Requirements</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1.1. Identification of Applicable legislation and Contractual requirements</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1.2. Intellectual property rights</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1.3. Protection of Records</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1.4. Privacy and protection of personally identifiable information</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>20.1.5. Regulation of cryptographic controls</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>20.2. Information Security Reviews</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>20.2.1. Independent Review of Information Security</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>20.2.2. Compliance with security policies and standards</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>20.2.3. Technical compliance review</td>
<td>65</td>
<td></td>
</tr>
</tbody>
</table>
**Abbreviations**

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMP</td>
<td>Advanced Malware Protection</td>
</tr>
<tr>
<td>BCC</td>
<td>Bangladesh Computer Council</td>
</tr>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BSTI</td>
<td>Bangladesh Standards and Testing Institution</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-circuit television</td>
</tr>
<tr>
<td>CPTU</td>
<td>Central Procurement Technical Unit</td>
</tr>
<tr>
<td>DC</td>
<td>Data Center</td>
</tr>
<tr>
<td>DG</td>
<td>Director General</td>
</tr>
<tr>
<td>DRS</td>
<td>Disaster Recovery Site</td>
</tr>
<tr>
<td>e-GP</td>
<td>Electronic Government Procurement</td>
</tr>
<tr>
<td>GoBiSM</td>
<td>Government of Bangladesh Information Security Manual</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, Ventilation, and Air Conditioning</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
<tr>
<td>IMED</td>
<td>Implementation Monitoring and Evaluation Division</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPR</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>IPS</td>
<td>Intrusion Prevention System</td>
</tr>
<tr>
<td>IS</td>
<td>Information Security</td>
</tr>
<tr>
<td>ISSC</td>
<td>Information Security Steering Committee</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>MIN</td>
<td>Media Identification Number</td>
</tr>
<tr>
<td>MoU</td>
<td>Memorandum of Understanding</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>NGFW</td>
<td>Next-generation firewall</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operations Center</td>
</tr>
<tr>
<td>NTP</td>
<td>Network Time Protocol</td>
</tr>
<tr>
<td>O&amp;M</td>
<td>Operations and Management</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OWASP</td>
<td>Open Web Application Security Project</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PE</td>
<td>Procuring Entity</td>
</tr>
<tr>
<td>PHI</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>RPO</td>
<td>Recovery Point Objective</td>
</tr>
<tr>
<td>RTO</td>
<td>Recovery Time Objective</td>
</tr>
<tr>
<td>SOD</td>
<td>Segregation of Duties</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UAT</td>
<td>User Acceptance Testing</td>
</tr>
<tr>
<td>UPS</td>
<td>Uninterruptible Power Supply</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-site scripting</td>
</tr>
</tbody>
</table>
Definition

(1) **Asset**: Anything that carries value to CPTU.

(2) **Attack**: Attempt to destroy, expose, alter, disable, steal, sabotage, eavesdropping, gain unauthorized access to or make unauthorized use of CPTU’s asset.

(3) **Authentication**: Provision of assurance that a claimed characteristic of an entity is correct.

(4) **Availability**: e-GP System up and running online available to users at any given or specified point of time and being accessible and usable upon demand by authorized entities.

(5) **Business Continuity**: Processes or Procedures for ensuring continued business operations (e-GP operations).

(6) **Confidentiality**: Information stored in e-GP system is not made available or disclosed to unauthorized individuals, entities, systems or processes.

(7) **Classified Information**: It refers to the categories of information classified in accordance with the Security Regulations.

(8) **Control**: Managing risk in e-GP system by implementing policies, procedures, processes, devices etc., which can be of administrative, technical, management related, or legal nature. Control is also used as a synonym for safeguard or countermeasure.

(9) **Control objective**: Statement describing what is to be achieved as a result of implementing controls.
(10) **Corrective action:** Action to eliminate the cause of a detected nonconformity or other undesirable situation.

(11) **Eavesdropping:** An unauthorized access to information through a network attack by capturing packets while communication/transmission of data or information.

(12) **Exploit:** A technique or code that uses a vulnerability to provide system access to the attacker.

(13) **Guideline:** A description that clarifies what should be done and how, to achieve the objectives set out in policies information processing facilities any information processing system, service or infrastructure, or the physical locations housing them.

(14) **Information System:** An electronic information system that processes data electronically through the use of information technology - including but is not limited to: software, database, computer systems, servers, workstations, terminals, storage media, communication devices, network resources, and internet.

(15) **Integrity:** When authorized persons are allowed to make changes to the information stored or processed by Information Systems in any aspects.

(16) **Information security:** Preservation of confidentiality, integrity and availability of information ensuring authenticity, accountability, non-repudiation, and reliability.

(17) **Information Security (IS) Policy:** A documented list of management decisions and instructions that describe in detail
the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction.

(18) **Information security event:** An information security event is 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.

(19) **Information security incident:** An information security incident 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.

(20) **Policy:** Overall intention and direction as formally expressed by management.

(21) **Risk analysis:** Systematic use of information to identify sources of risk and to estimate the impact of the risk.

(22) **Risk assessment:** Overall process of risk analysis and risk evaluation.

(23) **Risk evaluation:** Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
1. Introduction

Information and Communication Technology (ICT) is of paramount importance in e-GP (Electronic Government Procurement) system that transforms manual procurement process into an electronic procurement process. This involves not only the applications to ensure business control, but also comprises necessary software, hardware, database management system, data center, human interactions, and many other IT equipment. Management and control of such assets is essentially important to provide the best possible services to e-GP users and thus make the organization sustainable.

Security of e-GP system managed by the Central Procurement Technical Unit (CPTU) is highly important as the Government has declared e-GP as one of the critical government infrastructures. Confidentiality, Integrity and Availability of the system shall be maintained at all times through controls that are commensurate with the criticality of e-GP, so as to protect the system from all types of threats - internal or external, deliberate or accidental. It shall also be ensured that all legal, regulatory, statutory and contractual obligations are met.

The policy outlines the Information Security domains that are designed to meet e-GP system’s Information Security objectives and mitigate business risks. The policy provides management direction and support to implement information security as per ISO 27001:2013 standard. Moreover the policies defined in this document are also in line with GoBISM (Government of Bangladesh Information Security Manual) and Information Security Policy Guideline (Government gazette, 6th April 2014 by ICT Division).
2. **Objective**

The Information Security Policy defines necessary control requirements to ensure management and control of e-GP system protecting against damage, destruction, unauthorized disclosure or changes, whether it is accidental or deliberate. The policy complies with relevant laws and regulations of Bangladesh.

Information Security Policy of e-GP has the following objectives:

- To protect government and stakeholder’s data and information asset by safeguarding its confidentiality, integrity and availability;

- To ensure smooth operations of e-GP system by safeguarding its confidentiality, integrity, availability and competitiveness;

- To establish controls for protecting data and information resources from theft, abuse, misuse or any form of damage;

- To encourage management, staff, individual consultants, Operations and Management firms, third-party vendors to maintain an appropriate level of awareness, knowledge and skills allowing them to minimize the occurrence and severity of Information Security Incidents;

- To ensure that e-GP continues its operational activities in the event of significant data and Information Security Incidents;

- To promote e-GP system security culture in e-GP management.
3. Applicability and Scope

The security policies and standards contained in this document have been established to cover business processes, information and data, software, hardware and networks used by the e-GP system and its users/stakeholders.

This security policy of the e-GP shall apply to any person (management, employees, administrators, contractors, O&M firms and third-parties including general visitors to the e-GP system) who access information using e-GP system or any other system related to e-GP in particular, the security policy applies to the following information assets belongs to e-GP:

- Any proprietary information;
- Personnel information relating to the employees of CPTU;
- All client's (i.e. Procuring Entities, Bidders etc.) data and information;
- All supplier, contractor and other third-party information;
- All hard copy documents;
- All software assets such as application software, system software, development tools and utilities acquired and maintained;
- All physical assets, such as computer equipment, communications equipment, media and equipment;
- All utilities/services, such as power, lighting, HVAC associated with e-GP.
Furthermore, the policy is applicable to

- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, O&M firms and their employees, vendors etc.) of CPTU and other individuals, entities or organizations that have access to e-GP systems;

- All locations where users have access to various ICT Assets and ICT Services including locations that have secure areas providing critical ICT Assets and ICT Services;

- All ICT Assets and ICT Services involving data, applications, network, security devices, servers and other ICT system that needs to be appropriately protected from physical and environmental threats;

- All Service Providers who render their ICT services to e-GP and have access to e-GP facilities (i.e. DC, DR, Other sites).
4. Data and Information Asset

4.1. Definition

CPTU considers data and information as the important asset which is operationally, administratively, commercially and personally significant and have value to CPTU and other stakeholders. CPTU has fundamental ‘duty of care’ and legal obligation to protect e-GP data and information asset from unauthorized or accidental modification, loss, damages or release.

4.2. Forms of data and information

a) Documents and papers (hard copy of the application, documents etc.);

b) Electronic data stored in e-GP system;

c) The system (software, hardware and networks) on which the information is stored, processed or communicated;

d) Intellectual information (knowledge or perceptions) acquired by e-GP;

e) Physical items from which information regarding design, components or use could be derived; and

f) Images, Audio or Video clips related to e-GP data

4.3. Asset Classification

All e-GP assets (i.e. data, software, hardware, networks etc.) shall be classified for assigning access level. Information resources need to be identified, characteristics analyzed, and then classified. e-GP assets include in general:

a) Databases and data files, system documentation including process, research information, user manuals, training materials, operational or support procedures, business continuity plans, fallback arrangement, audit trails, and archived information;

b) Application software, system software, development tools, and utilities;

c) Computer equipment, communication equipment, removable media, and other equipment;

d) Computing and communications services;
e) People, and their qualifications, skills, and experience:

f) Intangibles, such as reputation and image of e-GP:

g) Contracts and agreements:

h) Data stored in e-GP system.

Information stored in e-GP system may have different form of presence; it can have different states as well. Such as:

a) Archived Information:

b) PE. Bidder documents stored in database or tape drive or in any media:

c) Regular tender information processed in applications:

 d) Communication/ correspondence and perception:

e) Information that travels through internet:

Different security mechanism shall be applied considering the importance of the information and classifying information as required.

e-GP assets shall be classified in terms of its characteristics, value, legal requirements, sensitivity and criticality. Following three (3) levels of information classification shall be defined and applied for the classification of the e-GP assets:

1) Confidential - This classification shall apply to sensitive assets that are intended for use within CPTU/Authorized users. Its unauthorised disclosure could adversely impact on reputation and operations of e-GP system and the users and possesses high risks. For example Password, Bid price, encrypted data etc.

2) Restricted - This classification shall apply to sensitive assets that are intended for use within CPTU/Authorized users. Its unauthorised disclosure/misuse could cause serious impact on e-GP system and its users and possesses medium risks. For example access to data centre equipment, bidders information, bid evaluation etc.
3) Public or Unclassified- This classification shall apply to all documents and information that has been published to the public domain. For example tender advertisement, Notification of awards etc.

All assets shall be handled according to the classification levels to ensure security of the information resource.

Risk classification shall be done for all assets to enable CPTU to focus on asset protection mechanisms on assets that are most susceptible to specific risks.

4.4. Information Owner

The information owner is a functional owner responsible for ensuring information classification with different state, proper controls to address confidentiality, integrity, authenticity and availability of information. Information owner has authority and responsibility for controlling production, development, maintenance, using security controls over the asset; placing appropriate level of protection, reviewing the information classification, security controls, access restriction periodically for making cost-benefit decisions essential to ensure accomplishment of organizational objectives. Considering the definition, Director General (DG), CPTU or the delegated officer will be the owner of e-GP system.

4.5. Information Custodian

The information custodian will be designated personnel by the owner to be responsible for protecting information by maintaining safeguards and controls established by the owner; he/she will take prior approval if necessary before sharing any information. Senior System Analyst or the delegated officer will be the information custodian for e-GP system.
5. Leadership

5.1. Leadership and commitment

A committee i.e. “Information Security Steering Committee (ISSC)” chaired by DG, CPTU or the delegated officer shall be formulated to drive the information security initiatives with a top-down approach.

The ISSC shall perform the following activities:

a) Ensuring that information security objectives are identified, CPTU’s requirements are met and are integrated in relevant processes;

b) Reviewing and approving Information Security policies and overall responsibilities;

c) Assessing, accepting and sponsoring the security controls;

d) Authorizing any new information processing facilities;

e) Top management coordination and reporting;

f) Segregation of Duties (SOD);

g) Allocation of roles and responsibilities to individuals;

h) Accountability of information security management;

i) Incident reporting and mitigation;

j) Organize Security awareness and training

Information security co-ordination shall involve co-operation by representatives from different stakeholders of CPTU with relevant roles and job functions. The Information Security Steering Committee shall comprise of nominated members by DG, CPTU or the delegated officer.

The ISSC shall undertake the following operational activities:

1. Initiating plans and programs to maintain information security awareness on a continuous basis;

2. Ensuring adequate resources are available for maintaining information
security;
3. Ensuring that the implementation of information security controls is coordinated across all the locations (i.e. DC, DR, other locations identified by CPTU);
4. Monitoring significant changes in the exposure of information assets to major threats;
5. Reviewing and monitoring major security incidents;
6. Ensuring all appropriate information security controls are implemented for all new information processing facilities installed;
7. Reviewing the effectiveness of the implementation of the information security policy;
8. Providing clear direction and visibility to the management with respect to security initiatives;
9. Identifying the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the organization.

The ISSC shall meet at least once a quarter to assess the security requirements of e–GP. The Minutes of Meeting (MOM), with the attendance details shall be documented. The MOM shall be circulated to all the members of ISSC irrespective of attendance along with the measurable action points.

5.2. Policy

5.2.1. Purpose

The purpose of this document is to define policies that need to be adopted in order to maintain the confidentiality, integrity, and availability of e–GP and to ensure the secure delivery of services.

5.2.2. Policy statement

Central Procurement Technical Unit (CPTU) shall ensure the safety of the data, continuity of critical network services to deliver uninterrupted e-GP services while abiding to legal and regulatory obligations by developing, implementing and continually improving business continuity management system.
5.2.3. Implementation

The ISSC is accountable for the overall information security of e-GP. The information security policy shall be approved by the Honorable Minister of Planning. The approved policy shall be published and communicated to all stakeholders. The operations and management functions are responsible for implementing information security and shall be responsible to implement the relevant rules and to communicate it to the relevant staff.

5.2.4. Document owner

The owner of the Information Security Policy is the Senior System Analyst or the delegated officer, who shall be responsible for the maintenance and update of the policy document.

5.2.5. Document convention

The following two keywords used within this document to indicate the level of requirements:

1. SHALL – Mandatory to follow. Failure to comply with the requirements may be construed as non-compliance to the policy.

2. SHALL NOT – Non-use of this control is mandatory. Failure to comply with the requirements may be construed as non-compliance to the policy.

5.2.6. Document distribution

CPTU shall distribute the document to all relevant stakeholders related to e-GP (i.e. Government officials, Consultants, O&M firms, Third-party vendors, donors etc.) for the compliance with the policy. Compliance to e-GP Information Security Policy shall be mandatory. Chairperson of ISSC, shall ensure continuous compliance to this policy through regular audit and monitoring.

5.2.7. Violation of the policy

Any individuals/firm found to have violated this Information Security Policy shall be a subject to disciplinary action as per the law of the land up to and including termination of employment/contract.
5.2.8. Waiver criteria

Requested waivers shall be formally submitted to DG, CPTU or the delegated officer including justification and benefits attributed to the waiver for approval. Senior System Analyst or the delegated officer shall assess if minimum security requirements have been met before the approval of any waivers. The waiver shall only be used in exceptional situations for communicating non-compliance with the policy for a specific period of time as per requirements of the waiver requested. Waiver shall not be applicable for e-GP data. All waivers granted shall be assessed for any vulnerabilities/ risks to CPTU information assets. Compensating controls for the identified vulnerabilities / risks shall be implemented and monitored on a continuous basis. At the completion of the time period, the need for the waiver shall be reassessed and re-approved, if necessary.
6. Planning

6.1. Actions to address risks and opportunities

6.1.1. General

When planning for information security, CPTU shall consider the organisational security issues and the requirements of various stakeholders. CPTU shall determine the risks and opportunities that need to be addressed to:

1. Ensure that information security initiatives can achieve their intended outcome;
2. Prevent or reduce undesired effects; and
3. Achieve continual improvement.

CPTU shall plan:

1. Actions to address these risks and opportunities; and
2. The integration and implementation of these actions information securities processes and evaluate the effectiveness of these actions.

6.1.2. Information security risk assessment

CPTU shall identify risks associated with the assets and apply relevant controls to mitigate the risks.

Analyse information security risks:

a) The information risk assessment process shall assess the potential consequences that would result if the risks identified were to materialize (i.e. impact),

b) The realistic likelihood of the occurrence of these risks shall be assessed;

c) The level of risk shall be determined.

d) To predict what-if scenarios and risk assessment using Data Analytics and AI.

Moreover, regular vulnerability analysis and risk assessment shall be conducted by CPTU’s internal team and submit the report to ISSC.
### 6.1.3. Information security risk treatment

Following table indicates the identified risks and applied controls to mitigate them:

<table>
<thead>
<tr>
<th>Asset group</th>
<th>Threat</th>
<th>Probability of Occurrence</th>
<th>Impact</th>
<th>Level of Risk</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/Storage</td>
<td>Virus/Malware attack</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>End point protection, patch management, Firewall.</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Physical security, password protection, Monitoring</td>
</tr>
<tr>
<td></td>
<td>Power failure</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Alternate power supply</td>
</tr>
<tr>
<td></td>
<td>Natural disaster</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Redundancy, Business Continuity Plan</td>
</tr>
<tr>
<td></td>
<td>Fraud and theft</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Physical security, redundancy, Audit</td>
</tr>
<tr>
<td></td>
<td>Fire</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Fire extinguisher, Alarm</td>
</tr>
<tr>
<td>Communication channels and network equipment</td>
<td>Unauthorized access</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Physical security, password protection, Monitoring</td>
</tr>
<tr>
<td></td>
<td>Power failure</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Alternate power supply</td>
</tr>
<tr>
<td></td>
<td>Natural disaster</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Redundancy, Business Continuity Plan</td>
</tr>
<tr>
<td></td>
<td>Fraud and theft</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Physical security, redundancy, Audit</td>
</tr>
<tr>
<td></td>
<td>Fire</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Fire extinguisher, Alarm</td>
</tr>
<tr>
<td></td>
<td>Incident by mistake</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Segregation of duties, Supervision, Formal approval</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Asset group</th>
<th>Threat</th>
<th>Probability of Occurrence</th>
<th>Impact</th>
<th>Level of Risk</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>End users (Laptops, PCs, Hand held devices)</td>
<td>Virus/Malware attack</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>End point protection, Firewall</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Password, Firewall, static IPs</td>
</tr>
<tr>
<td>Software (Application/third-party)</td>
<td>Vulnerabilities</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>Patching, Development, Firewall</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access to source code</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Physical security, Access control, Version management</td>
</tr>
<tr>
<td></td>
<td>Incident by mistake</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Code review, Quality assurance</td>
</tr>
<tr>
<td>Data/Information</td>
<td>Virus/Malware attack</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>End point protection, Firewall</td>
</tr>
<tr>
<td></td>
<td>Unauthorized access</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Web application firewall, Log monitoring, Network traffic monitoring, Encryption at the transmission layer</td>
</tr>
<tr>
<td></td>
<td>Natural disaster</td>
<td>Low</td>
<td>High</td>
<td>High</td>
<td>Backup, Business Continuity Plan</td>
</tr>
<tr>
<td></td>
<td>Fraud and theft</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Log monitoring, Firewall, Encryption</td>
</tr>
<tr>
<td></td>
<td>Unavailable due to server/network problem</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Redundancy, Backup</td>
</tr>
</tbody>
</table>
6.1.4. Information security objectives and planning to achieve them

CPTU shall establish information security objectives at relevant functions and levels. The information security objectives shall:

1. Be consistent with the information security policy;
2. Be measurable;
3. Consider applicable information security requirements, and results from risk assessment and risk treatment;
4. Be communicated; and
5. Be updated as appropriate.
7. Implementation of Information Security Policy

Policy Statement

Security of information assets of e-GP is of paramount importance. Confidentiality, Integrity and Availability of these assets shall be maintained at all times through controls that are commensurate to the criticality of the asset, so as to protect the assets from all types of threats, whether internal or external, deliberate or accidental.

Control Objectives

CPTU shall strive to safeguard Confidentiality, Integrity, and Availability of the information systems and resources in e-GP’s facilities by:

1. Setting up, maintaining, continually monitoring and improving an effective Information Security Management framework;

2. Taking corrective and preventive actions for security incidents/breaches with respect to Information Security Policy;

3. Conduct periodic Risk Assessment;

4. Creating security awareness for internal and external stakeholders;

5. Ensuring continuous improvement and effectiveness of the information security framework.

7.1 Management Direction for Information Security

To provide management direction and support for information security in accordance with CPTU business requirements and relevant applicable laws.

7.1.1. Policies for information security

1. CPTU Information security policy shall be approved by the management;

2. Approved security policy shall be published and communicated to all relevant stakeholders.

7.1.2. Review of policy for Information security

1. The Information Security Policy shall be reviewed annually and at the time of any major change(s) proposed and agreed by the ISSC.
8. Information Security Organization

Policy Statement

The Information Security Steering Committee (ISSC) defines the authority and responsibilities to manage information security for e-GP. The Committee will ensure structured co-ordination of information security related activities within CPTU.

Control Objective

The Committee establishes a management framework to ensure that information security is given oversight, managed, understood, communicated and implemented at the right level across CPTU to meet compliance and to set security rules.

8.1 Internal Organization

DG, CPTU or the delegated officer shall form a management framework for Information Security Steering Committee (i.e. ISSC) to implement and monitor the information security controls within CPTU. DG, CPTU or the delegated officer will decide the number of members of the committee.

8.1.1 Information Security Committee Roles and Responsibilities

Chairperson

The Chairperson of Information Security Committee shall have the following responsibilities:

1. Accountable for overall execution of information security policy of e-GP system;

2. Responsible for driving technology and service decisions to ensure compliance and protection of data & ICT assets related to e-GP;

3. Managements of strategic and operational risks;

4. Review the effectiveness of the information security policy.

Members

The members will have the following responsibilities:

1. Manage the overall Information Security program for e-GP system;

2. Responsible for developing and maintaining the security policies, procedures and standards for e-GP;

3. Ensure that all critical operations are carried out in accordance with the security requirements;
4. Review external audit reports and assess the recommended controls;
5. Manage the response to any information security incidents;
6. Perform regular audits and provides regular reports;
7. Analyse the security incidents and document corrective and preventive action and escalation.

**Authorization of New Information Processing Facility**

Any new information processing facility that would be a part of e-GP shall be compliant with the documented policies and procedures. The following shall be the role of ISSC as a part of authorization process of new information processing facility:

1. The policies and procedures pertaining to use of information resources shall be implemented;

2. Review of the implementation of Information Security Policy (including Physical and logical controls) shall be assessed before the new information processing facility is authorized.

**8.1.2 Segregation of Duties (SOD)**

1. There shall be an Organization Chart for ICT personnel working in e-GP;
2. Duties and areas of responsibilities for each personnel of Procuring Entities (PEs) and CPTU related to e-GP ICT system shall be documented and published;
3. Segregation of duties shall be established to prevent unauthorized or unintentional modification or misuse of the information assets and shall be maintained and reviewed time to time;
4. Fall-back plans for various levels of system support personnel shall be formulated, maintained and reviewed time to time by CPTU;
5. Monitoring of activities, audit trails, logs, management supervision and independent reviews shall be implemented and reported on regular basis;
6. Exceptions to segregation of duties shall be documented and approved by DG, CPTU or the delegated officer.

**8.1.3 Contact with Authorities**

1. CPTU shall maintain contact with authorities including but not limited to BCC (Bangladesh Computer Council), law enforcement authorities, fire department,
BSTI (Bangladesh Standards and Testing Institution) and other emergency services;

2. The contact details of these agencies shall be maintained and displayed at prominent places in the CPTU office location.

8.1.4 Contact with Special Interest Groups

1. CPTU shall maintain contact with special interest groups and authorized information security forums for receiving and distributing updates on new vulnerabilities, security threats, regulations and/or risks pertaining to the services and information systems used in the CPTU.

8.1.5 Information security in project management

1. Information security should be addressed in all the new development initiatives of e-GP, regardless of the type of the development (i.e. software, datacenter enhancement etc.);

2. All the initiatives shall comply with the requirements of the Information Security Policy;

3. Project Risk Assessment and risk mitigation plan must be done at the initiation stage of the project.

8.1.6 Portable Devices and Telecommuting

8.1.6.1 Portable device policy

Information Security controls shall be deployed to safeguard and prevent leakage of information through portable devices (CPTU’s property) such as laptops and handheld devices. Controls are:

1. No CPTU equipment shall be connected to non-CPTU networks without authorized approvals;

2. Physical protection, encryption for information in storage and transfer, back-up of data and virus protection of devices shall be ensured;

3. In case of loss and theft of devices containing sensitive information, the user shall inform CPTU administration in the form of written document (email or SMS or Letter) within 24 hours:
4. Training sessions shall be conducted for the employees to increase awareness on the risks.

8.1.6.2 Telecommuting

Controls shall be established and implemented to maintain the Confidentiality, Integrity and Availability of the CPTU Information for teleworking requirements:

1. There shall be a secure communication channel between the teleworkers and the CPTU network (i.e. VPN with authorized device/IP, TeamViewer, WebEx, etc.);

2. Teleworkers shall get written approval from DG, CPTU or the delegated officer to use the network.


9. Human Resources

Policy Statement

Information security controls shall be designed and integrated in the Human Resources (HR) processes to ensure that employees understand their responsibilities in maintaining confidentiality, integrity and availability of information assets.

Control Objective

These controls define the information security requirements that need to be incorporated in the recruitment processes, employment and transfer/exit of employees to reduce the risk of theft, fraud and misuse of CPTU’s assets and facilities.

9.1 Prior to Employment

1. Information Security responsibilities shall be addressed during recruitment and included in the employment contracts. Potential recruits might be screened before recruitment depending upon the roles assigned to the resource.

2. All vendors, consultants and sub-consultants, O&M firms, third-party vendors and service providers appointed by CPTU shall sign a confidentiality (non-disclosure) agreement.

9.1.1 Screening

1. The background verification report shall capture any of the following:
   a) Character references checks including criminal record verification; and/or
   b) Evidence of enquiry with previous employer.

9.1.2 Terms and conditions of employment

CPTU shall ensure that the Terms and Conditions of employment reflect the information security requirements and include the following:

1. The employee shall sign a Non-Disclosure agreement;

2. The exclusive rights to patents, copyrights, inventions or other intellectual property developed by the employees shall be with CPTU.
9.2 During Employment

9.2.1 Management Responsibilities
All employees, O&M firms, third-party vendors and service providers shall implement and comply with the information security policy in accordance with established guideline and procedures of the Bangladesh Government.

9.2.2 Information Security awareness, education & training
1. Employees of CPTU, O&M firms and third-party vendors shall receive regular updates on organizational security policies and procedures.

2. Recurring information security awareness activities shall be performed to ensure that the behavior of staff is in accordance with the policy and rules. Consultants, O&M firms, Third-party vendors shall assure that their employees follow the policy accordingly.

3. Records shall be maintained for all the awareness activities.

4. CPTU shall arrange training for the employees of CPTU in home and abroad to keep them updated on information security.

9.2.3 Disciplinary process
1. Disciplinary action on violating information security policy shall be as per the law/act of the Government of Bangladesh.

2. All employees shall be made aware of such law/act.

9.3 Termination and change of employment

9.3.1 Termination or change of employment responsibilities
1. CPTU employees, consultants, O&M firms, third-party vendors and service providers shall be governed as per Government rules and regulations or the contract agreement;

2. A termination process shall include returns of all issued assets that are the property of CPTU and sign-off from DG, CPTU or the delegated officer;

3. The employee user ID, credentials and access rights shall be revoked/deactivated at the end of the last working day.
10. Assets Management

Policy Statement

All e-GP assets shall be classified and managed based on their confidentiality, sensitivity value and availability requirements. The level of security to be accorded shall depend directly on the classification level associated with each asset.

Control Objective

To establish controls for protecting information assets. Information Assets shall be identified, inventoried, labelled, classified, accounted for and shall have comprehensive protection based on the criticality of the asset.

10.1 Responsibility for Assets

All critical information assets (i.e. data, business applications, operating systems, databases, network, third-party utility software, etc.) shall be identified and be documented in a register that shall be kept up-to-date.

CPTU shall be responsible for:

a) Ensuring that assets under e-GP system are classified as per classification policy;

b) Ensuring that periodic validation of the asset inventory is in place.

10.1.1 Inventory of Assets

CPTU shall identify and document all the information assets related to e-GP system in the Asset Register. The information on the Asset Register shall contain, at a minimum, the following information about each of the assets:

1. The type and location of asset,
2. Date of Registration
3. The User,
4. The classification of the asset,
5. The Confidentiality, Integrity and Availability (CIA) ratings of the information asset.
6. The overall criticality rating for each of the identified information asset.
10.1.2 Ownership of Assets

All assets (i.e. software, hardware, networks, storage, data etc.) under e-GP system are the property of Bangladesh Government.

10.1.3 Acceptable use of Assets

Any users using the information assets or accessing the information processing facilities shall follow the ‘acceptable use of assets’ as mentioned below:

1. All PCs, laptops and workstations shall be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or by logging-off when the host will be unattended;

2. Users are responsible for exercising good judgment regarding the reasonableness of personal use of any asset given to them by CPTU for official use. In such case, CPTU encourages using the asset for official use only rather than personal use. The internet shall not be used to access offensive or illegal material, such as material containing racist terminology or nudity. Nevertheless, protection of assets (i.e. PC, Laptop, Phone etc.) from any types of threats (i.e. Physical threats – theft, lost etc. and Technical threats – virus, data loss etc.) are the sole responsibility of the user;

3. Users shall use latest and licensed anti-malware software (i.e. antivirus) for protecting the assets under their possession;

4. Users shall keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. If the user thinks the password has been compromised, he/she should change the password immediately;

5. Users shall not open e-mail attachments received from unknown senders, which may contain viruses;

6. For security and network maintenance purposes, authorized individuals within CPTU may monitor equipment, systems and network traffic at any time;

7. CPTU reserves the right to audit networks and systems on a periodic basis to ensure compliance with the Information Security Policy. The periodic audit can be conducted by internal resources of CPTU or any third-party resources;

8. CPTU reserves the right to use the Open Source software/tools duly authorized by CPTU’s ISSC for e-GP system’s operational purposes;
9. CPTU reserve the right to perform any kind data analysis on e-GP data stored in the database for enhancement of e-GP system, research, and new service offerings.

**Besides, the following activities are, implicitly strictly PROHIBITED**

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property rights, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by CPTU;

2. Exporting data, application software, e-GP application source code (full or in part), technical information, technical documentation, encryption software or technology etc. on external media;

3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.);

4. Revealing the account password to others or allowing use of individual’s account by others. This includes family and other household members when work is being done at home;

5. Using CPTU computing asset to actively engage in procuring or transmitting material that is in violation of the law of Bangladesh;

6. Attempting security breaches or disruptions of internal (inside CPTU) or external (outside CPTU) network communication. Security breaches include, but not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. On the other hand, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes (i.e. any types of hacking activities);

7. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam); and

8. Any form of offensive communication via email, telephone, whether through language, frequency, or size of messages.

Users must be cautious on using the CPTU assets by abiding the law of Bangladesh.
10.1.4 Return of Assets

CPTU shall ensure that at the time of termination/change of employment/contract, change in the responsibilities or transfer of employee, end of contract, all the assets belonging to CPTU are returned by the employees/consultants/O&M firms/vendors.

10.2 Information Classification

CPTU shall ensure that all assets receive protection in accordance with their value, criticality, sensitivity and legal implications based on the criteria of Confidentiality, Integrity and Availability.

10.2.1 Labeling of Information

The assets shall be labeled and secured based on the classification, from the time it is created until the time it is destroyed or disposed. The labels shall be pasted on all media holding any information (hard copies, CD-ROMs, etc.) and also on all other assets (Physical and Electronic).

10.2.2 Handling of Assets

Information assets handling procedures including the secure processing, storage, transmission, and destruction shall be followed for each classification level. Retention period for all records shall be complying to the legal and/or mission requirements.

Addition/Changes of Information Assets

1. New information assets deployed shall have all the required features and functionalities that comply with CPTU’s information security requirements;

2. All information assets, operations and services shall be subjected to change management (14.1.2) controls.

10.3 Media Handling

CPTU shall ensure there is no unauthorized disclosure, modification, removal or destruction of information stored on media used in e-GP system.

10.3.1 Management of removable media

Records shall be maintained for all removable media used in e-GP system.

1. Removable media shall be sanitized before it is issued to the user:
2. The contents of any re-usable media shall be made unrecoverable before putting it to re-use.

3. Records shall be maintained for the issuance and return of removable media:

4. If removable media are required to be taken out of office premises, user shall get authorization from the CPTU:

5. Removable media containing critical data (i.e. database backup, configuration backup etc.) shall be kept encrypted. Decryption key and recovery key shall be shared with CPTU;

6. Removable media containing critical data (i.e. database backup, configuration backup, etc.) must have Media Identification Number (MIN) and record should be maintained for all the media with MIN containing critical data;

7. User shall not transfer any Personally Identifiable Information (PII) from removable media to any personal device;

8. In the event of loss of removable media, the user shall inform CPTU immediately.

10.3.2 Disposal of media

1. Media containing critical and sensitive information shall be disposed-off in a secure manner or as per the contractual agreement with the respective third-parties;

2. The technique used for disposal shall depend on the type of media and the classification of information that is contained in the media;

3. Disposal of media/information shall be done by authorized users under supervision of ISSC and a record shall be maintained;

4. The contents of any re-usable media that are to be removed shall be erased or destroyed physically to prevent reuse;

5. The media containing sensitive information like tape cartridge, hard disk, CD, USB, etc. should be physically damaged under the supervision of ISSC in such a way that data cannot recovered at all applying any recovery techniques;
6. The media containing sensitive information like paper should cross-shredded or burned during disposal under the supervision of ISSC.

10.3.3 Physical media transfer

1. In case of shipment or movement, the removable media must have media identification number (MIN) - shall be recorded and protected in signed and sealed envelope and sent through an approved courier service or hand delivered;

2. It shall be ensured that the third-parties involved in the transfer, signs an agreement ensuring required security of information assets;

3. CPTU employees and third-party staff carrying media are required to ensure its protection during transit via tamper proof envelop/box and encryption.
11. Access Control

Policy statement
Access control is applied to protect the e-GP information systems from unauthorized access, modification, disclosure or destruction. Access shall be given need to access need to know basis as per business requirement.

Control Objective
To define controls need to be implemented and maintained in order to protect e-GP information systems against unauthorized access.

11.1. Business Requirement for access control

11.1.1. Access Control Policy
An access control policy shall be documented, implemented and reviewed to control access to e-GP information and systems, to keep information available when needed and restricting unauthorized access and intentional/unintentional damages.

11.1.2. Access to Networks and Network Services
1. User access to network shall be monitored and controlled as per acceptable use policy (10.1.3);
2. Only authorized users shall be granted in CPTU network;
3. Separate network shall be created for guest use;
4. Separate System Administration Network shall be created to administer the system using privilege password. System administration network must not be connected with the internet to protect privilege accounts from the potential cyber threats;
5. User login to the network shall be controlled/monitored centrally.

11.2. User Access Control Management

11.2.1. User Registration and De-registration
The ‘User’ registration, modification and de-registration, for granting/revoking access to all information systems shall be done in accordance with the defined Access Control Matrix and e-GP guideline.
11.2.2. User Access Provisioning

1. eGP users (Procuring Entity, Tenderers etc.) shall follow the eGP guideline or registration process to register in the system:

2. Access to the users providing technical support to eGP system shall be granted as per the requirement and following the Access Control Matrix.

11.2.3. Management of Privilege Access Rights

1. Privilege levels associated with each type of operating system, applications, database, and network resources shall be identified and documented;

2. Privileges shall be allocated to individuals based on their roles and responsibilities after approval from DG, CPTU or the delegated officer.

11.2.4. Management of Secret Authentication Information of Users

Allocation of secret authentication information shall be controlled through the following:

1. Users shall be forced to change their own password on first use;

2. User identity shall be verified prior to reissue of password and acknowledgement shall be obtained via e-Mail/SMS;

3. Default vendor password/credentials shall be changed following installation of new systems or software.

11.2.5. Review of User Access Rights

User access rights shall be reviewed by ISSC twice a year.

11.2.6. Removal or Adjustment of Access Rights

CPTU shall ensure that, in case of any change in the responsibilities of the user, the access rights are revoked or modified as required.


11.3. User Responsibilities

11.3.1. Use of Secret Authentication Information

1. All users with access to information assets shall be responsible for maintaining effective access controls, particularly regarding the use of passwords and access to the system;
2. Violation of Information Security Policy is a severe offence and may subject to termination from the job/contract or disciplinary action;
3. Sharing of Password is a violation of Information Security Policy and may subject to termination from the job/contract or disciplinary action.

11.4. System and Application Access Control

11.4.1. Information Access Restriction

1. Access to information and application systems shall be on “need-to-know” basis;
2. Access rights to e-GP system shall be reviewed at periodic intervals (twice a year) by ISSC.

11.4.2. Secure Log-on Procedure

The operating systems of servers, workstations and/or network devices shall be controlled through a secure log-on like:

1. System or application identifiers shall not be displayed until the log-on process has been successfully completed;
2. Display a general notice warning that the equipment should only be accessed by authorized users;
3. Users shall log off/sign out from the system once the job is done.

11.4.3. Password Management System

1. The allocation of initial passwords shall be done in a secure manner and these passwords shall be changed at first logon;
2. All User passwords (including administrator passwords) shall remain confidential and not to be shared, posted or otherwise divulged in any manner;
3. CPTU shall force strict password rules to comply with the password management policy mentioned below;

31
General:

All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.) shall be changed on at least every 90 days;

All user-level passwords used to access emails, web accounts, laptops, desktop computers etc. shall be changed at least every 90 days;

System-level passwords shall not be communicated through email messages or other forms of electronic communication;

All user-level and system-level passwords shall conform to the guidelines described below.

Guideline:

A. General Password Construction Guidelines

The common uses of password are user level accounts, web accounts, email accounts etc. Since password is the only way to authenticate, every user shall choose a strong password for himself/herself.

Strong password has the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+--=\{|\};':",<>?,/)
- At least eight alphanumeric characters long.
- Not a word in any language, slang, dialect, jargon, etc.
- Not based on personal information, names of family, etc.

B. Password Protection Standards

Users SHALL NOT use the same password for various access needs. For example, user should select one password for the email account and a separate password for the laptop.

Users SHALL NOT share passwords with anyone, including administrative assistants (i.e. Help desk, e-GP admin etc.). All passwords are to be treated as sensitive and confidential assets.
Users:

- Shall not reveal any password over the phone to ANYONE;
- Shall not reveal any password in an email message;
- Shall not reveal his/her password to the superiors/supervisors;
- Shall not talk about the password in front of others;
- Shall not hint at the format of a password (e.g., "my favorite color");
- Shall not reveal a password on questionnaires or security forms or in a letter;
- Shall not share a password with family members;
- Shall not reveal a password to co-workers while on vacation;
- Shall not use the "Remember Password" feature of applications (e.g., Browser, MS Outlook etc.);
- Shall not write passwords down and store them anywhere in the office;
- Shall not store passwords in a file on ANY computer system (including tablets or similar devices);
- If an account or password is suspected to have been compromised, report the incident to CPTU and change the password.

C. Application Development Standards

Applications:

- Shall support authentication of individual users, not groups;
- Shall not store passwords in clear text or in any easily reversible form;
- Shall provide authentication management, such that one user cannot take over the functions of another.

11.4.4. Use of Privileged Utility Program

1. The use of utility programs that might be capable of overriding system and application security controls shall be restricted and controlled;
2. Vendor default utilities shall be disabled during new server or network device commissioning.
11.4.5. Access Control to Program Source Code

1. Access to the source code of e-GP systems shall be controlled to prevent any corruption of the application programs;

2. Consultants shall have restricted access to program source libraries;

3. All updates or issue of the program sources to developers shall be carried out through an authorized request.

11.4.6. Secure Coding Practice

CPTU shall ensure that internal or external team/developers shall follow the below practices while developing any application for CPTU to ensure best possible security of the system:

1. The developers shall follow standard security guidelines, (i.e but not limited to OWASP - www.owasp.org and secure coding guideline published by BCC) on developing the application (i.e. web portal, mobile app etc.);

2. The developers shall address common web application vulnerabilities such as SQL Injection, Cross Site Scripting (XSS), Broken authentication and Session management etc. (considering the OWASP top ten vulnerabilities) and ensure that the application is free from such vulnerabilities;

3. CPTU shall ensure that the vulnerability assessment is being done and corrective measures have been taken based on the assessment before the final release of the application.

11.4.7 Database access policy

1. Access shall be restricted in production database based on the job nature and need basis.

2. Direct access to raw data in Database is strictly restricted with exception in case of unavoidable minor corrections required in Database where an authorized person of CPTU is required to access directly in database must have prior approval from DG, CPTU or the delegated officer and corrections to be made in presence of another staff from CPTU as double checker. DG, CPTU or the delegated officer shall issue an office order for this authorization. Standard scripts shall be developed to make
such corrections. CPTU shall keep audit trail for each changes. Subsequently CPTU shall take all necessary steps to avoid direct access to database. A separate change request module shall be developed to make this changes through interfaces:

3. Day to day activities shall be supported by relevant audit log;

4. DBA (Database administrators) shall access to production database for maintenance purpose only;

5. Person assigned for administration i.e Database backup, health monitoring, cluster health, High Availability group, performance tuning etc. shall not have read/write permission to production data;

6. CPTU shall enforce a clear SOD for database maintenance and operation;

7. CPTU shall use Role-Based-Access-Control (RBAC) model to access the database following the concept of Role with different users having different security permissions.
12. Cryptography

Policy Statement

CPTU shall provide adequate protection to its information and information systems with cryptographic controls.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA shall be used for data encryption.

The use of proprietary encryption algorithms is not encouraged for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by ISSC.

Control Objective

The objectives of Cryptographic policy are to establish and implement controls to maintain the confidentiality, integrity and availability of information and ensure non-repudiation.

12.1. Cryptographic Controls

12.1.1. Policy on Use of Cryptographic Controls

Cryptographic controls shall be used in compliance with all relevant contracts, agreements, laws, and regulations. However, it is important to use current version of cryptographic protocols (i.e. TLS/SSL, SSH etc.)

12.1.2. Key management

The key management for secure key generation, ownership, distribution, archival, storage and revocation shall be performed to protect the keys throughout their lifecycle.

The cryptographic keys shall be protected against unauthorised modification, substitution, unintended destruction and loss.
13. Physical and Environmental Security

Policy Statement

CPTU shall provide adequate protection to its information systems and facilities against unauthorized physical access and environmental threats. Controls shall be implemented to maintain the physical and environment security of all assets of e-GP system.

Control Objective

The Physical and Environmental Security policy defines security controls required to protect information assets and information processing facilities of e-GP system from unauthorized access and physical and environmental threats.

13.1. Physical Security Perimeter

e-GP system’s security perimeter shall cover all e-GP facilities (i.e. Office premises, Data center, Mirror site and Disaster recovery site). Physical security controls shall be implemented in all those sites.

13.1.1. Physical Entry Controls

1. Only persons authorized by CPTU shall be allowed to enter the facilities by showing valid identification;

2. The facilities shall be under CCTV coverage along with biometric door lock; The CCTV recording must be available at least for six months;

3. Visitors’ entry into the facilities shall be restricted. Security validations and checks such as verifying the identity of the visitor, checking the belongings and bags, making entry in visitor register shall be carried out;

4. Any third-party support activities inside these facilities shall be accompanied by authorized CPTU personnel;

5. A MoU shall be signed with any third-party managing physical security of any of the facilities.

13.1.2. Securing the Facilities

1. All e-GP facilities shall remain secured during and after office hours or when unattended:
2. Lockable cabinets or safes shall be provided in the offices, rooms and information processing facilities;
3. Fire doors and extinguishing systems shall be installed, monitored, and tested regularly.

13.1.3. Visitor Management

1. Reception areas shall be manned by a receptionist(s) and/or security guard(s) during the office hours to track and control visitor movement;
2. Visitor shall be accompanied by authorized CPTU personnel during his/her visit in the data center or information processing facilities;
3. Entry and exit along with date, time and the purpose of visit of visitors shall be recorded and maintained at the entry points.

13.1.4. Protecting Against external and environmental threats

All c-GP facilities shall implement controls to protect information assets and facilities against damage from environmental threats like fire, flood, lightning, earthquake & terrorist attacks, explosion, civil unrest and other forms of manmade/natural threats.

13.1.5. Working in Secure Areas

Datacenter, Network Operations Center (NOC) room shall be identified as restricted area and security controls (i.e. Glass doors, biometric lock, CCTV etc.) shall be implemented to prevent intrusion and damage to these areas.

13.1.6. Delivery and Loading Areas

NOC (Network Operations Center) room shall be used for loading/unloading new equipment and troubleshooting purposes, otherwise loading/unloading area shall be chosen where CCTV coverage is available.

13.2. Equipment Security

13.2.1. Equipment Siting & Protection

1. c-GP facilities shall be located away from hazardous processes or materials;
2. Uninterrupted and auxiliary power supplies shall be provided to c-GP facilities;
3. Protection shall be provided to e-GP facilities against damage from exposure to water, smoke, fire, dust, chemicals, electrical supply interference and other environmental hazards etc.

13.2.2. Supporting Utilities

All equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities by using online UPS and Generator.

13.2.3. Cabling Security

Channels shall be used to protect power and network cables from unauthorized interception or damage.

13.2.4. Equipment Maintenance

All equipment shall be maintained to ensure continued availability and integrity for uninterrupted business. DR site will be maintained and tested regularly to handle any uneven situation.

13.2.5. Removal of Assets

Any equipment, information, information systems, storage devices and/or software owned by CPTU can be removed from e-GP facilities only after written approval from DG, CPTU or the delegated officer.

13.2.6. Security of Equipment and Assets Off-Premises

Each user, carrying/managing the portable devices/equipment such as laptops, handhelds and other mobile devices that is owned by CPTU or having e-GP’s information, shall be responsible for the security of that respective equipment.

13.2.7. Secure disposal or re-use of equipment

1. All information/data and licensed software shall be removed or securely overwritten prior to the decommissioning of any equipment containing e-GP information;

2. Destruction/disposal of media shall be done in accordance with media disposal policy.
13.2.8. *Unattended user equipment*

1. Users shall terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

2. Users shall log-off from applications or network services when no longer needed;

3. Users shall secure computers or mobile devices from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use;

4. All the desktops and laptops connected with the CPTU network and e-GP system should prompt for password to get access to system if the desktops/laptops remain inactive for the period of 5 (five) minutes.

13.2.9. *Clear desk and clear screen policy*

Users shall follow clear desk and clear screen policy for e-GP facilities to reduce risks of unauthorized access and loss of and damage to information:

1. Users shall lock away (ideally in a safe or cabinet or other forms of security furniture) sensitive or critical information, e.g on paper or on electronic storage media, when not required, especially when the office is vacated;

2. Computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password when unattended and should be protected by key locks or passwords when not in use;

3. Unauthorized use of photocopiers and other reproduction technology (e.g. scanners, digital cameras) shall be prohibited;

4. Media containing sensitive or classified information should be removed from printers immediately.
14. Operations Security

Policy Statement

CPTU shall ensure effective and secure operation of its information systems and computing devices. Controls shall be implemented to protect the information contained in and processed by these information systems and computing devices.

Control Objective

To ensure timely and controlled resolution of IT incidents and prevent unauthorized access, misuse or failure of the information systems and processing facilities of e-GP system.

14.1. Operating Procedures and Responsibilities

14.1.1. Documented operating procedures

Standard Operating Procedure (SOP) shall be developed every time new information system or services are introduced. The SOP shall include the necessary activities to be carried out for the operation and maintenance of the system or service and the actions to be taken in the event of a failure.

14.1.2. Change Management

Any changes in e-GP system including patch update, modification/enhancement update/release must be tested in Test environment and proper User Acceptance Testing (UAT) has to be done before applying it into the production environment. Any changes in e-GP system and its facilities shall be done according to the following procedure:

CPTU shall:

1. Identify and record of significant changes;
2. Plan ahead and test the changes before final release/implementation;
3. Assess the potential impacts, including information security impacts of such changes;
4. Collect formal approval from DG, CPTU or the delegated officer for proposed changes;
5. Verify information security requirements have been met;
6. Communicate of change details to all relevant stakeholders;
7. Plan fall-back procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events;
8. Keep provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident;
9. Any changes in the system should be deployed by system administration team as per the documentation provided by the software development team and Original Equipment Manufacturer (OEM) like Microsoft, Red Hat, Cisco, HP, Dell, IBM, Huawei etc.

After changes are made, a report containing all relevant information should be updated, maintained and retained until the next system and security audit is conducted.

14.1.3. Capacity Management

1. CPTU shall conduct schedule system tuning and monitoring to ensure and, where necessary, improve the availability and efficiency of systems;
2. CPTU shall introduce detective controls to indicate problems in due time;
3. CPTU shall implement system management and monitoring tools.

14.1.4. Segregation of Duties in Operational Procedures

1. CPTU shall ensure separation of duties in all technical and operational procedure;
2. CPTU must ensure Segregation of Duties (SOD) in Operating System administration, application (e-GP) administration, database administration, network administration and cyber security management in e-GP Operations;
3. Development team should not have access to production environment (application and database) to ensure the integrity and confidentiality of the system unless such access provided by the permission of the DG, CPTU or the delegated officer in writing in case of special needs. Such access shall be fully documented and records shall be maintained.

14.1.5. Separation of Test and Production Facilities

The Test and Production facilities / environments shall be physically and/or logically separated.
14.1.6. Exchange of Information

To prevent loss, modification, destruction, or misuse of information, CPTU shall protect and control exchange of critical business information assets and software with third parties and outside organization.

14.1.7. Publicly Available Information

Any e~GP information that need to be made publicly available for public consumption shall be identified, verified and approved by authorities before making it public.

14.1.8. Patch Management

1. Patches to the production systems shall be applied as per OEM’s (Original Equipment Manufacturer) instruction to ensure that the systems are protected against the threats from the spread of viruses, worms and malicious activities to an acceptable level;

2. A central patch management system shall be established for applying patches to the information systems;

3. Before deploying any patches, roll back options shall be made available;

4. Proper backup of the system shall be taken before deploying the patch;

5. System availability shall be the highest priority while deploying the patches. Proper precaution shall be taken;

6. All the security patches must be deployed in the system within 30 (thirty) days of release of security patches;

7. Security patches include but not limited to operating system (OS), application, database, network equipment, servers and storage firmware upgrade, etc.

14.2. Protection from Vulnerabilities including Malware

14.2.1. Controls against malware

1. Detection, prevention and recovery controls shall be implemented in all information systems to protect against malicious software/malware;

2. CPTU shall implement NGFW (Next Generation Firewall) with AMP (Advanced Malware Protection), End point protection, Intrusion detection and prevention system, web application firewall and other necessary controls to address the latest vulnerabilities and insecurities that could bring the system down or result in information disclosure or destruction.
14.3. Backup

14.3.1. Information Backup

1. CPTU shall maintain Backup register that contains complete records of the backup copies such as Site location, Device type, Name, Backup type, frequency, Backup location, date etc.;
2. CPTU shall follow 3-2-1 backup rule i.e. take at least three copies of the data, store the copies on two different media and keep one backup copy offsite;
3. CPTU shall ensure an appropriate level of physical and environmental protection on the backup;
4. For critical data (i.e. Application, DB etc.), CPTU shall test the backup quarterly to ensure that they can be relied upon for emergency use when necessary;
5. Backup kept any external media shall be encrypted;
6. For database, log shipping in 15 minutes interval shall be applied besides regular data backup.

14.4. Logging and Monitoring

eGP facilities shall be monitored through CCTV and information security events shall be recorded. This policy details that logs shall be used to ensure information system problems are identified.

14.4.1. Event logging

1. CPTU shall ensure that the event logs recording the critical user-activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring;
2. Regular monitoring of the audit log shall take place and results shall be recorded;
3. Logs shall be monitored and analyzed for any possible unauthorized use of information systems;
4. Access to audit trails and event logs shall be provided to authorized personnel only.
14.4.2. Audit Logging

1. Audit logs recording user activities, exceptions, and information security events shall be produced and kept until the next audit is performed to assist in future investigations and access control monitoring.
2. Procedures shall be implemented for monitoring system use to ensure that users are only performing processes that have been explicitly authorised.

14.4.3. System Monitoring

1. Systems shall be monitored and information security events shall be recorded to ensure conformity to access policy and standards.
2. Monitoring of system use shall be in line with the various policies and procedures that are part of the Information Security Management System and any other critical activities.

14.4.4. Protection of Log Information

1. Logging facilities and log information shall be protected against tampering and unauthorised access.
2. Logs shall be protected from unauthorised access or deletion.

14.4.5. Administrator and operator logs

1. Information systems shall be configured in such a way that the system administrator and system operator activities are logged.
2. Users shall not have access rights to access administrator and operator logs.
3. Administrator and operator logs shall be reviewed at specified intervals.

14.4.6. Clock synchronization

CPTU shall synchronize the clock of all servers, network and communication equipment with the time servers - bsti.time.gov.bd and bsti2.time.gov.bd through an NTP (Network Time Protocol) server maintained by Bangladesh Standards and Testing Institutions (BSTI). However, in case of failure to communicate to BSTI servers, the time of active directory of the datacenter will prevail.
14.5. Control of Operational Software

14.5.1. Installation of software on operational systems

1. Updating of the operational software, applications and program libraries shall be performed by authorized administrator(s) upon authorization from DG CPTU or the delegated officer;
2. Operational systems shall only hold approved executable code and not development code or compilers;
3. Applications and operating system software shall only be implemented after successful testing; the tests shall cover usability, security, effects on other systems and user-friendliness and shall be carried out on staging or test environment; CPTU shall ensure that all corresponding program source libraries have been updated;
4. A rollback strategy shall be in place before changes are implemented;
5. An audit log shall be maintained of all updates to operational program libraries;
6. Previous versions of application software should be retained as a contingency measure.

14.6. Technical Vulnerability Management

14.6.1. Management of Technical Vulnerabilities

1. Vulnerability assessments including penetration testing and application security testing shall be performed on an on-going basis by CPTU’s internal security team;
2. Assessment report shall be submitted to ISSC on a quarterly basis;
3. The administrator(s) (database, application, system) shall configure the database and other critical servers based upon requirement of CPTU;
4. Administrator(s) shall ensure that the servers are hardened as per baseline security standards (i.e. GoBISM etc.);
5. Administrator(s) shall patch the server with latest patches and ensure all critical security patches are installed;
6. Administrator(s) shall install anti-virus, anti-malware and other necessary security software required and mandated by CPTU;
7. Administrator(s) shall enforce policies on the server. Administrative users should be enabled only for troubleshooting purposes;
8. System administrator shall ensure logging is enabled for the database server and audit trail is maintained;
9. Database administrator should install the database software on the server and configure it against minimum baseline security standard of CPTU;
10. All default username should be removed and disabled for database and underlying system;
11. Database administrator shall ensure appropriate logging is enabled for database and audit trail is maintained for user and administrative activities;
12. Database users shall be given minimum privileges required to perform their task;
13. Database views should be enabled and enforced where required;
14. Database administrator shall ensure that database software is patched and updated;
15. Database administrator shall disable all the unnecessary services of the database, all necessary services should be documented;
16. The database server shall follow system acquisition and deployment process when deployed in production environment;
17. Database administrator in consultation with system administrator shall identify criticality of database and provide backup requirement to backup team;
18. Network administrator shall ensure that only services (ports) necessary for database server shall be allowed on firewall;
19. Network administrator, if required, will provide remote access to database administrators on database administrator after necessary approvals;
20. Network administrator shall provide remote access via VPN or other secure network protocols;
21. Insecure remote access to database server shall be disabled even from the CPTU’s internal network.

14.6.2. Restriction on Software Installations

1. CPTU shall define and restrict which software shall be installed by users on the computer systems (i.e. Application whitelisting);
2. Only Licensed software shall be installed.
3. Open source software/tools shall be authorized by ISSC after testing for usage.
14.7. Information system audit consideration

14.7.1. Information systems audit controls

1. Audit requirements on the operational systems shall be planned, documented and agreed in order to minimise the risk of disruptions to business processes;

2. CPTU shall ensure that the persons carrying out audit shall be explicitly identified and be independent of the activities audited.
15. Communications Security

Policy Statement

CPTU shall ensure effective and secure communication of information.

Control Objective

The objectives of this policy are to:

1. Ensure protection of information during its transmission from CPTU to eGP users and vice versa;
2. Protect the confidentiality, integrity and availability of eGP information assets from the adverse impact of malicious code.

15.1. Network Security Management

CPTU shall develop and implement network security systems and procedures, and provide network security resources (Firewall, IDS, etc.) to protect the eGP information assets from unauthorized or illegal access.

15.1.1. Network Control

1. All connections initiated from outside to CPTU networks and vice versa shall be routed and controlled through firewalls positioned at the network boundaries;
2. The access rules of firewalls shall be maintained only by respective personnel responsible for firewall administration;
3. IPS and IDS shall be implemented.

Network Routing Control

Shared networks shall have routing controls to ensure that computer network and information flows do not breach the access control policy and network access and security policy of CPTU.

Limitation of Connection Time

Administrative sessions in servers and network devices shall be specified to disconnect the connection after 10 minutes of idle time.
15.1.2. Security of network services

1. Security features, service levels and management requirements of all IT network services included in network services agreement shall be identified;
2. Non-essential services shall be disabled on all information systems.

15.1.3. Segregation in Networks

The security of CPTU network shall be divided into separate logical network domains. Each of these domains shall be protected by a defined security perimeter. All required Network Zones and Data Flow Access Controls shall be designed and documented.

System management (privilege users/system administrators) network should be separate from the CPTU users network. System management network should not have access to internet.

15.2. Information Transfer

15.2.1. Information transfer policy and Procedures

1. Procedures shall be documented to ensure controls (such as technical controls, contracts/ agreements) implemented to exchange business information with stakeholders, third-parties and within CPTU;
2. Employees shall exchange the information as per c-GP information classification guidelines.

15.2.2. Agreement on Information transfer

1. Agreement for the exchange of information between CPTU and all stakeholders shall be established;
2. Agreements shall include, but not limited to the following:
   a) Management responsibilities for controlling and notifying storage, transmission and disposal of information;
   b) Procedures to ensure traceability and non-repudiation;
   c) Ownership and responsibilities for data protection, copyright and software license compliance.
15.2.3. Electronic Messaging

1. Technical controls shall be designed and implemented to prevent unauthorized interception, modification and interruption of the information transmitted through email system;
2. Formal training shall be conducted for all employees for the acceptable use of email system;
3. All messages generated by email shall be considered the property of CPTU;
4. Shall contain a disclaimer message approved by CPTU.

Acceptable use of email system

All email communication should be encrypted.

Prohibited Use

The e-GP email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users who receive any emails with this content from any other CPTU user should report the matter to their supervisor immediately.

Monitoring

CPTU employees shall have no expectation of privacy in anything they store, send or receive on the email system. CPTU management may monitor messages without prior notice.

Email Retention Policy

Administrative Correspondence (5 years)
Fiscal Correspondence (5 years)
General Correspondence (5 years)
Ephemeral Correspondence (Retain until read, destroy)

Recovering Deleted Email via Backup Media

CPTU shall maintain backup from the email server to any external encrypted device from where it can be recovered as and when required (in shortest time).
15.2.4. Confidentiality or non-disclosure agreements

Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements shall be applicable to external parties or employees of CPTU.

Confidentiality and non-disclosure agreements shall comply with all applicable laws and regulations of Bangladesh.
16. System Acquisition, Development and Maintenance

Policy Statement

Security controls shall be integrated during acquisition, development, deployment and maintenance of the application software, system software, products and/or services ensuring confidentiality, integrity and availability of the eGP information.

Control Objective

The aim of this policy is to ensure that security is an integral part of the eGP system and all security requirements are identified.


16.1.1. Information Security Requirement Analysis and Specification

1. Security requirements shall be analysed and necessary controls be introduced in case of any enhancements to eGP application;
2. All new information systems or services that are acquired, developed or enhanced shall undergo security assessment, to ensure that security controls are incorporated in them.

16.1.2. Securing application services on public networks

1. Adequate security controls as per applicable laws shall be put in place to ensure the confidentiality, integrity and availability of the eGP information contained in the publicly available systems;
2. Prior to deployment, all publicly available systems i.e. website, web services, mobile apps etc. shall be tested and it shall be ensured that the identified vulnerabilities are fixed prior to publishing any information in such systems.

16.1.3. Protecting application services transactions

1. Information involved in application services transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay via SSL/TLS encryption (the updated and latest one);
2. A secure communications channel shall be setup between all involved parties for application services transactions;
3. All aspects of application services transactions and communications shall be encrypted.

16.2. Security in Development and Support Processes

16.2.1. Secure Development Policy

Secure development shall be followed to build up a secure service, architecture, software and system considering security of the development environment, security requirements in the design phase, security check points within the project milestones, security in version control and likewise.

16.2.2. System Change Control Procedure

1. Formal change management procedures (14.1.2) shall be enforced in order to minimize the adverse impact on the system;
2. Introduction of new systems and major changes to existing systems shall follow a formal process of documentation, specification, testing, quality control, and managed implementation;
3. Changes shall not be carried out in operational environment directly.

16.2.3. Technical review of applications after operating platform changes

1. New releases/Patches pertaining to the operating system shall be tested before being implemented in the operational environment to ensure that there is no adverse impact on operation, application controls or security;
2. The application controls shall be reviewed to ensure that they have not been compromised by the operating system changes.

16.2.4. Restrictions on changes to software packages

1. Vendor-supplied software packages shall not be modified as far as possible without consulting the vendor;
2. Any requirement for change to such software shall be controlled and shall follow the CPTU change management procedure.

16.2.5. Secure system engineering principles

Secure information system engineering principles shall be designed into all architecture layers:

1. Business
2. Data
3. Applications,
4. Technology

New technology shall be analyzed for security risks and the design shall be reviewed against known attack patterns.

16.2.6. Secure development environment

CPTU shall assess risks associated with system development and establish secure development environments.

16.2.7. Outsourced development

1. For the customized software developed by third-parties, arrangements pertaining to licensing, code ownership and intellectual property rights shall be documented in the contract between CPTU and the third-parties.
2. Testing of the software shall be done before its installation to detect malicious code;
3. CPTU will obtain and retain vulnerability assessment and remediation report from any third-party vendor before production deployment.

16.2.8. System security testing

Testing shall be conducted from security perspective during the development phase. The tests shall be conducted against the security requirements identified in the planning phase and the vulnerabilities, which can be exploited by internal/external threat source.

16.2.9. System acceptance testing

1. Acceptance criteria for new information systems and information processing facilities, upgrades and new versions shall be defined;
2. Tests of the systems shall be carried out during development and prior to actual production;
3. Security clearance shall be obtained before any new information systems, upgrades and/or new versions are accepted;
4. User Acceptance Testing (UAT) shall be conducted prior to the deployment of the systems in the production environment.
16.3. Test Data

16.3.1. Protection of test data

1. Acceptance tests shall be carried out using the test data, which shall be similar to the operational data.
2. The development team shall ensure that test data is secured and sanitized during testing.
3. Test data shall be securely backed up at different stages of testing.
4. Production data shall not be used for testing purposes.
17. Supplier Relationships

Policy Statement

All measures shall be considered to ensure that the data/information or information processing facilities accessed by third-party/vendor/supplier/O&M firms is secured.

Control Objective

The objective of the Supplier Relationships policy is to:

1. Minimise the adverse impact on e-GP assets from suppliers;
2. Ensure relevant Security Processes are established with the suppliers;
3. Document clauses for security in the supplier contracts.

17.1. Information security in Supplier relationships

17.1.1. Information Security Policy for Supplier relationship

The Supplier Relationship policy shall address the following clauses:

1. All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for e-GP information.
2. Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
3. CPTU shall ensure the right to monitor, review and audit the supplier/vendor or any third-party providing service delivery.

17.1.2. Addressing security within supplier agreements

Agreements with third-parties involving accessing, processing and communicating of e-GP information shall cover all relevant security requirements.

1. If the third-party sub-contracts any service/work, the sub-contracted parties and their employees shall also adhere to the policy;
2. Description of the information to be provided or accessed and methods of providing or accessing the information shall be identified.
3. Legal and regulatory requirements, including data protection, intellectual property rights and copyright, are met;
4. Training and awareness requirements are identified for specific procedures and information security requirements;
5. Service Levels, including related to security, as defined in the agreements shall be monitored and reported;
6. Third-parties shall be subjected to independent reviews by CPTU.

17.1.3. Information and communication technology supply chain

Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and supply chain.

17.2. Supplier Service Delivery management

17.2.1. Monitoring and review of supplier services

1. Service reports and evidences provided by the third-parties shall be reviewed at regular intervals;
2. Audits shall be conducted at specified intervals to assess the compliance of third-parties with the agreed contracts and the clauses incorporated in the contracts;
3. Review of third-party audit trails and records of security incidents, operational problems, failures, fault logging and disruptions shall be done regularly;
4. Identified problems/ issues shall be managed and resolved with the supplier/third-party;
5. All third-parties shall audit their respective subcontracting agencies on a periodic basis and ensure compliance to the security policy.

17.2.2. Managing changes to supplier services

1. Management shall review all third-party contracts/ agreements annually or whenever the contracts are renewed;
2. Changes to the contracts with third-parties/ suppliers shall be reviewed and approved in accordance with the Information Security Policy;
3. Acknowledgement for adhering to any revised policies shall be taken from the third-parties within the defined timelines of its release.
18. Information Security Incident Management

Policy Statement

The Information Security Incident Management Process shall ensure that all reported security breaches and violations are reported, responded to promptly and acted upon to prevent recurrence.

Control Objective

To ensure information security events and weaknesses associated with e-GP business applications, systems and infrastructure are communicated in a manner that allows timely corrective action to be taken and minimize adverse impact of the incident.

18.1. Management of information security incidents and improvements

18.1.1. Responsibilities and Procedures

The aim of this process is to provide a set of guidelines that provide a basis for consistent decision-making with respect to Incident Management.

18.1.2. Reporting information security events

1. Employees shall be adequately trained for identification and reporting of security incidents.

2. Employees of CPTU and third-party vendors shall be made aware of procedures for reporting a security incident. All reported incidents shall be logged and classified according to predefined criteria.

3. CPTU shall implement procedures for detecting, reporting and responding to incidents.

18.1.3. Reporting information security Weaknesses

It is the responsibility of all employees and third-party/vendor/s to note and report any observed or suspected information security weaknesses in systems or services to CPTU by email, phone or any other documented format. CPTU will record and monitor the mitigation process of such events.
18.1.4. Assessment of and decision on information security events

Reported incidents shall be assessed to verify if these shall be reported as security incidents. Classification and prioritization of an incident shall help to identify the impact and extent of an incident.

18.1.5. Response to information security incidents

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties.

The response shall include the following:

a) Collecting evidence as soon as possible after the occurrence;

b) Escalation, as required;

c) Ensuring that all involved response activities are properly logged for later analysis;

d) Communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

e) Dealing with information security weakness(es) found to cause or contribute to the incident;

f) Once the incident has been successfully dealt with, formally closing and recording it. Post-incident analysis shall take place, as necessary, to identify the source of the incident.

18.1.6. Learning from Information Security Incidents

CPTU shall establish a knowledge repository for the information gained from the evaluation of all information security incidents.

18.1.7. Collection of Evidence

1. Where a follow-up action against a person or organization after an information security incident involves legal action, (either civil or criminal) evidences shall be collected, maintained and presented to the relevant authorities.
2. Internal procedures shall be developed and followed when collecting and presenting evidences for the purpose of disciplinary action handled within an organization.

3. Forensic investigation methods shall be applied, whenever required, to collect evidence in the course of investigation of information security incidents.

4. Records shall be maintained for all security incidents and stored in a manner to prevent unauthorized access or modification.

Policy Statement

Application systems and business processes that are critical to the CPTU shall be planned for continuity of operations in the events of disaster.

Control Objective

To counteract interruptions to e-GP business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

19.1. Information Security Continuity

19.1.1. Planning Information Security Continuity

1. A comprehensive Business Continuity Plan (BCP) that includes RTO (Recovery time objective) and RPO (Recovery Point Objective) shall be developed and implemented in order to maintain or restore business operations in the required time scales;

2. Business Continuity Plan shall be developed based on critical processes present in the e-GP system and related assets through Business Impact Analysis;

3. Business Impact Analysis shall evaluate the impact of the interruptions in terms of damage and recovery period and identification of risk and threats affecting e-GP.

19.1.2. Implementing information security continuity

1. CPTU shall ensure that the business continuity plan defines the responsibilities of respective teams at the time of a business continuity event;

2. The plan shall be tested on bi-annual basis and shall be updated to incorporate the changes in business environment and technology infrastructure of e-GP system;

3. Detailed technical recovery procedure shall be documented as part of DR and tested periodically;
4. CPTU shall define the methodology to list down steps on documentation and implementation of business continuity framework;

5. CPTU shall ensure the maximum availability of the security control during any adverse situation (i.e. disaster).

19.1.3. Verify, review and evaluate information security continuity

1. All plans documented as part of the business continuity framework shall be tested and exercised on an ongoing basis to ensure their effectiveness.

2. BCP shall be tested bi-annually to identify incorrect assumptions, oversights or changes in equipment or personnel.

19.2. Redundancies

19.2.1. Availability of information processing facilities

1. CPTU shall identify business requirements for the availability of information systems;

2. Redundant components or architectures shall be considered to ensure availability;

3. Redundant information systems shall be tested to ensure the failover from one component to another component as intended, wherever applicable.
20. **Compliance Policy**

*Policy Statement*

CPTU shall ensure that all stakeholders comply with the information security policy.

*Control Objective*

To ensure that controls are implemented to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements and if breached then, to identify the same through audit process.

20.1. **Compliance with Legal and Contractual Requirements**

20.1.1. **Identification of Applicable legislation and Contractual requirements**

CPTU shall identify the legal requirements with respect to the services rendered at CPTU.

20.1.2. **Intellectual property rights**

Intellectual Property Rights (IPR) shall be included in all the contracts, and shall be implemented.

20.1.3. **Protection of Records**

1. CPTU’s organizational records relating to Information Security shall be protected and stored as per the law of Bangladesh;

2. The records shall be protected based on their relevance, classification, and importance and stored in a vault according to the requirement of media on which they shall be recorded.

20.1.4. **Privacy and protection of personally identifiable information**

1. The importance of privacy shall be communicated to all employees involved in the processing of Personally Identifiable Information (PII);

2. The data protection and privacy of PII against unauthorized access, transmission, publication, damage, use, modification, disclosure and impairment shall be ensured at CPTU by implementing technical and administrative controls;

3. Responsibility for handling PII and ensuring the awareness of the data protection principles shall be dealt with as per relevant legislation,
20.1.5. Regulation of cryptographic controls

1. Cryptographic controls shall be used in compliance with all relevant agreements, laws and regulations;
2. Procedure for compliance assurance shall be documented and maintained;
3. PII shall be secured and encrypted at all the locations of its storage and transmission in CPTU’s system.

20.2. Information Security Reviews

20.2.1. Independent Review of Information Security

1. Audit requirements on the operational systems shall be planned, documented and agreed in order to minimize the risk of disruptions to business processes;
2. CPTU shall ensure that the persons carrying out audit shall be explicitly identified and be independent of the activities audited.

20.2.2. Compliance with security policies and standards

1. Compliance checks against security policy shall be done bi-annually.

20.2.3. Technical compliance review

1. Review of Information Security controls shall be carried out bi-annually;
2. Independent Technical Compliance Review and Reporting shall be organized;
3. Control of Proprietary Software Copying shall be introduced;
4. Identification of Applicable Legislation;
5. Prevention of Misuse of Information Processing Facilities;
6. Collection of Evidence;
7. Compliance with Security Policy;
8. Factors that shall require regular reassessment.

END OF INFORMATION SECURITY POLICY