# COMMONWEALTH CORPORATION INFORMATION SECURITY POLICY

## I. INTRODUCTION

Commonwealth Corporation recognizes the growing threat of information and identity theft and continues to formulate and implement policies that take steps to safeguard information. This policy is designed to safeguard Information Assets, including but not limited to Personal Information (Defined in Section III Personal Information), and Confidential Information (Defined in Section III Confidential Information) that is collected, used, stored, disposed, or disseminated in the process of providing services. This policy should be used as a basis for creating training for each staff member and as a general guide for each employee. If anything in this policy is not clear, or individuals do not understand how this policy relates to their function, an employee should contact the Information Security Officer or their direct manager for clarification as each employee is responsible for maintaining the security of Information Assets (Defined in Section IV.7 ) used during their daily duties.

A strong security position is maintained through the application of security controls, data ownership responsibilities, and maintenance of the security infrastructure. This policy articulates requirements that assist management in defining a framework that establishes a secure environment. This framework provides the overarching structure for safeguarding information and Information Technology (IT) Resources, achieving confidentiality, integrity and availability of data and IT Resources used to manage the services provided by Commonwealth Corporation.

It is the responsibility of Commonwealth Corporation (CommCorp) to have controls in place and in effect that provide reasonable assurance that security objectives are addressed. CommCorp has the responsibility to exercise due diligence in the adoption of this framework and to achieve compliance with the overall information security goals of the Commonwealth including compliance with laws, regulations, policies and standards to which their technology resources and data, including but not limited to personal information, are subject.

The Information Security Policy (ISP) is the umbrella document defining CommCorp's security program and provides the foundation upon which security programs will be formulated and implemented by each division within CommCorp. The ISP is applicable to CommCorp, its employees, grantees and contractors. The ISP is constructed with policy statements supported by a high-level description of the implementation requirements for that policy. Divisions with business operations related to the activities described in this ISP have detailed procedures that are separately maintained[1].

## II. PURPOSE

The purpose of this policy is to detail the security goals and objectives in the protection of agency Information Assets (Defined in Section IV. 7), including but not limited to confidential (sensitive) information, personal information, Information Technology Resources and other information as a first step to creating specific programmatic policies, procedures and controls that protect the agency's Information Assets from all threats whether internal or external, deliberate or accidental. In addition to the three guiding principles of information security: confidentiality, integrity and availability (CIA), agencies must review the overall implementation of security controls against all applicable laws, regulations, policies and standards.

[1] Reference provided in section on related documents.

**III. SCOPE**

The policies referenced herein apply, but are not limited to, the protection of confidential (sensitive) information, personal information (as defined in Massachusetts General Laws Chapters 66A and 93H) and other information ( and the use of IT resources that contain any of the above mentioned information) that is collected, handled, stored, processed, disseminated, and disposed of by this corporation and by all employees, contractors, and contracted business partners of this corporation, and must be incorporated into all inter-agency and other contractual agreements entered into as of the issue of this policy.

***Personal Information***

Personal information (PI) is defined in the Security Freezes and Notification of Data Breaches Statute (Massachusetts General Laws 93H):

Resident's first name (or initial) and last name in combination with:-

- Social security number (SSN);
- Drivers license (or state issued i.d.) number; or
- Financial account number.

***Personal Data***

Personal data under Fair Information Practices Act (FIPA)

Any information which, because of name, identifying number, mark or description can be readily associated with a particular individual. (except information that is contained within a public record.)

***Confidential Information***

Confidential Information is defined as:

- Personal financial information;
- Competitive information from organizations (applications or proposals for grants or financing);
- Information CommCorp's clients deem to be confidential as part of contractual obligations;
- Wages and wage records for participants in programs administered by CommCorp.

**IV. POLICY**

It is the policy of this corporation to ensure that all information, including but not limited to Information Assets that are collected, used, maintained, or disseminated in the process of providing services to the public is protected from all threats whether internal or external, deliberate or accidental. The three major tenets of information security covered by this information security policy include:

***Confidentiality***

Confidentiality involves ensuring that information is only accessible to those authorized to access it and therefore preventing both deliberate and accidental unauthorized access to sensitive information, including but not limited to personal information.

***Integrity***

Integrity involves safeguarding the accuracy and completeness of information and processing methods and therefore requires preventing deliberate or accidental, partial or complete, destruction, or unauthorized modification, of either physical media containing electronic data, or electronic data.

### *Availability*

Availability means that information and associated assets shall be accessible to authorized users when required. The key assets which include but are not limited to computer systems, applications, networks, and associated environmental and power facilities must be appropriately resilient according to defined service levels which define availability requirements. Therefore, the agency must define and adhere to appropriate business continuity plans which serve to improve the availability of key assets.

### *Security Objectives and Policies*

The security objectives of the corporation are defined within the following policy. For each objective, the security policy which details the objective(s) is referenced.

**1 Information Security Management Program**: CommCorp has implemented an Information Security Management Program that represents the policies and controls implemented within CommCorp. The program provides both management and users with a detailed understanding of the goals, approach and implemented controls for securing the organization's Information Assets.

Requirements stated within this document have been developed in alignment with the Information Security Policies and Standards, the overarching requirements adopted by the Commonwealth (of Massachusetts) Chief Information Officer (CCIO).

In compliance with the Information Policies and Standards issued by the CCIO, this policy addresses:

1. Information Security Policies and Practices and related security objectives and controls,
2. Compliance with all Federal, State, and privacy laws, and information security laws and regulations to which CommCorp's information is subject,
3. Compliance with review and audit requirements,
4. Security breach notification requirements,
5. Training and outreach requirements,
6. Contractual obligations, and
7. Ongoing evaluation and maintenance and improvement, including self-audits of security controls.

**2 Risk Assessment**: CommCorp shall develop policies to identify, quantify and prioritize risks to Information Assets against operational and security objectives, and to design, implement and exercise controls that provide reasonable assurance that objectives will be met.

a) Identification of risk factors includes the evaluation of risks by considering the potential threats to the information and the IT Resources, including:
   i. Loss of the information or systems due to accident or malicious intent.
   ii. Loss of availability such as the system being unavailable for a period of time.
   iii. Unknown changes to the information or system so the information is no longer reliable.

b) Identification of threats includes the evaluation of the impact and likelihood of potential threat, including:
   i. Cost if each threat were to actually occur. Costs should be interpreted broadly to include money, resources, time and loss of reputation among others.
   ii. Evaluation of the probability of each threat occurring.

**3 Risk Treatment:** CommCorp shall monitor and evaluate the specific controls that must be implemented to meet the stated security objectives. This process identifies which security controls will be or are implemented and details their appropriateness.

**4 Statement of Applicability:** The policy lists CommCorp's information security control objectives, controls and adopted policies that are relevant and applicable to CommCorp's information security management program for all Information Assets.

**5 Security Policy, Policy Adoption and Documentation Review**: CommCorp has adopted the comprehensive information security policy detailed herein consistent with the Enterprise Information Security Policy of the Commonwealth as well as based on an evaluation of CommCorp's own business drivers. The policy provides management direction and support for information security in accordance with relevant laws and regulations. The information security policy shall be approved by the Information Security Officer, the President and management, and published and communicated to all employees and relevant external parties.

CommCorp shall review the Information Security Policy annually at a minimum. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies. CommCorp shall also review the policies if and when significant changes occur within the organization that may have an impact on the effectiveness of the policy.

**6 Organization of Information Security:** In order to maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by employees and on-site contractors, and third parties, CommCorp shall document the specific responsibilities of staff and third parties, including:

a) Management shall actively support security within the organization through clear direction, and acknowledgement of information security responsibilities;
b) Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed;
c) The organization's approach to managing information security and its implementation (i.e., control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur;
d) Ensuring that all applicable contractual agreements incorporate and support the security-based requirements;
e) The risks to the organization's information and IT Resources from business processes involving external parties shall be identified and appropriate controls implemented before granting access;
f) Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities shall cover all relevant security requirements.

**7 Asset Management:** To maintain appropriate protection of information assets, CommCorp shall implement controls for achieving the following:

a) All assets shall be clearly identified and an inventory of all important assets drawn up and maintained;

b) Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented through an IT Policy;
c) Apply appropriate classification to information to thereby ensure adequate application of controls to protect that information;
d) Apply label and handle information to thereby affect adequate application of controls to protect that information;

***Information Assets***

e) The term Information Assets includes both original and copies (hard copy and electronic) of documents that have been transported to other locations or reside on electronic media. Such media may include flash memory drives, mobile or external hard drives, laptop or desktop computers, CDs, cell phones, and PDAs – even if they are not owned or managed by CommCorp. For example, a document that constitutes a CommCorp information asset does not lose its character by being stored, accessed, or saved on an employee's home computer, and such asset falls under the same level of security and protection against disclosure as it would if it were physically located on a CommCorp device at the corporate offices.

**8 Staff and Contractor Access:** CommCorp shall ensure that employees, contractors and third party users understand their security responsibilities and have the requisite skills and knowledge to ensure the effective execution of the roles they are assigned to reduce the risk of unauthorized access, use or modification of Information Assets, including:

a) Risk assessment to determine applicable level of employee screening prior to and upon change in responsibility during employment;
b) Security awareness and training during employment;
c) Disablement of access rights to data systems after an extended period of inactivity;
d) Return of agency issued equipment and/or devices upon termination or change of employment;
e) Removal of access rights upon termination of employment.

**9 Physical and Environmental Security:** CommCorp shall secure against the unauthorized physical access, damage and interference to the corporation's premises and information assets including but not limited to personal information and IT Resources by implementing:

a) Facility access controls of IT Resources;
b) Equipment security, including protections to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access; [IT]
c) Visitor control;
d) Secure disposal or reuse of equipment;
e) Physical security for offices, rooms, and facilities shall be designed and applied; and
f) All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

**10 Communications and Operations Management:** CommCorp shall develop procedures for managing system activities associated with access to Information Assets including information and IT resources, modes of communication, and information processing by implementing procedures including:

a) Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented;
b) Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed policy;
c) Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit;
d) Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring;
e) Procedures for monitoring use of IT resources shall be established and the results of the monitoring activities reviewed regularly;
f) Logging facilities and log information shall be protected against tampering and unauthorized access;
g) System administrator and system operator activities shall be logged;
h) Faults shall be logged, analyzed, and appropriate action taken; and
i) The clocks of all relevant information processing systems within an organization or security domain shall be synchronized with an agreed accurate time source.

**11 Access Control:** CommCorp shall implement controls for authorized access to Information Assets, IT Resources, information processing facilities, and business processes on the basis of business and security requirements. Access control rules shall take into account existing policies for information dissemination and authorization with consideration for the application of:

a) Restricted and controlled allocation and use of privileges (“least privilege”), where individual has the “least privilege” or the least access necessary to do his/her job;
b) Wireless and remote access controls;
c) Separation of duties;
d) Controlled access and authentication to applications, systems and networks;
e) Disablement of access rights to data systems after an extended period of inactivity;
f) User account and session management, including a guest user policy for giving visitors access to IT Resources;
g) Allocation of passwords shall be controlled through a formal management process; and
h) Appropriate authentication methods shall be used to control access by remote users.

**12 Information Systems Acquisition Development and Maintenance:** CommCorp shall ensure that information security is an integral component to IT Resources from the onset of each project or acquisition through implementing:

a) Application and system security;
b) Configuration management;
c) Formal change control procedures to control the installation of software on operational systems;
d) Encryption and key management; and
e) Software maintenance including but not limited to upgrades, antivirus, patching and malware detection response systems.

**13 Information Security Incident Management:** CommCorp shall establish management responsibilities and procedures that result in a consistent, effective and orderly approach for addressing information security incidents, consistent with the Information Security Policies and Standards of the Commonwealth including:

a) Collection of evidence related to the incident as appropriate using the Information Security Incident Report included as Appendix B;
b) Reporting procedures including any and all statutory reporting requirements and reporting to the CommCorp Board of Directors/EOLWD;
c) Incident remediation; and
d) Minimum report logging procedures.

Where a follow-up action against a person or organization after an information security incident involves legal action, evidence shall be collected, retained, and presented appropriately.

**14 Business Continuity Management with respect to Information Assets:** CommCorp will document, implement and annually test business continuity plans including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters via the adoption of a continuity of operations plan, including a disaster recovery plan. Plans shall be developed and implemented to maintain or restore operations and ensure availability of information without compromising security at the required level and in the required time scales following interruption to, or failure of, critical business processes.

**15 Compliance:** CommCorp shall implement the security requirements of this policy, in addition to any state or federal law, regulatory, and/or contractual obligations to which their Information Assets and IT Resources are subject, including but not limited to:

a) Data protection and privacy, including the security and privacy of personal information, shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses;
b) Documented plans for all audit requirements and activities for information systems and assets, as appropriate;
**c)** Audit requirements and activities involving checks on operational systems shall be carefully planned and implemented to minimize the risk of disruptions to business processes; and
**d)** Results of self-audits at a minimum annually.

**16 Maintenance:** CommCorp shall implement a regular schedule by which the Information Security Management Program is reviewed for ongoing effectiveness. The corporation's ISP, including security policies, procedures, and other controls, shall be subject to an appropriate level of monitoring and evaluation. Changes to the components of the corporation's ISP will be subject to appropriate review and approval, and be adequately documented.

## V. ROLES AND RESPONSIBILITIES

The roles and responsibilities associated with implementation and compliance with this policy follow and cannot be delegated:

**Commonwealth Corporation President**
As the head of the corporation, the President is responsible for exercising due diligence in adoption of this framework to meet the obligations of CommCorp by ensuring that adequate security controls are in place and in effect to promote reasonable assurance of security control objectives that safeguard the Information Assets, including but not limited to personal information. The President shall:

a) Reasonably ensure that all IT systems and applications developed conform to this and all related policies, standards and procedures of the corporation and the Commonwealth;
b) Ensure communication, training and enforcement that support the security goals of CommCorp and the Commonwealth;
c) Ensure proper oversight over any third parties with access to information assets and IT resources;
d) Review and sign all corporation security programs, plans, self-audits and reports; and
e) Be responsible for ensuring compliance with all applicable laws, regulations and contractual obligations.

**Information Security Officer (ISO)**
The CommCorp Information Security Officer shall:

a) Ensure that the goals and requirements of the Information Security Policy are implemented and met;
b) Maintain all required documentation as specified in the information security policies, standards and procedures of the corporation and the Commonwealth;
c) Conduct self-audits and at a minimum annually document reasonable assurance that compliance with information security policies, standards and procedures has been achieved;
d) Coordinate the corporation's compliance with the requirements of applicable executive orders, federal and state laws and regulations, Commonwealth IT security standards and policies, and security-related contractual requirements; and
e) Sign all required agency security programs, plans, self-audits, and reports to attest to the accuracy of completeness of the submissions.

The Information Security Task Force (ISTF) will be formed for the first year through March 2011 to ensure implementation of the ISP and to ensure improvement in the implementation and compliance of the policy.

**Staff**
It is the responsibility of all staff (i.e., including but not limited to employees, contractors, etc) to do everything reasonable and within their power to ensure that this policy is adhered to. All security incidents shall be immediately reported to the Information Security Officer (ISO) per corporation policy. The ISO will promptly respond to reported security incidents, and appropriately document the incident according to the corporation's specified policy.

**Third parties**
Third parties must ensure that all IT systems and applications developed by or for CommCorp conform to this and other applicable Information Technology Policies, Standards and Procedures of the Commonwealth.

## VI. RELATED DOCUMENTS

CommCorp's Information Security Policy has been developed consistent with the Enterprise Information Security Policy (EISP) guidance issued by the Commonwealth Chief Information Officer and the Information Technology Division (ITD.) Primary references that were used in development of the Commonwealth's EISP include:

a) Massachusetts Executive Order 504, available at www.mass.gov/Agov3/docs/Executive%20Orders/executive_order_504.pdf
b) M.G.L., Ch 93H, Personal Information, www.mass.gov/legis/laws/mgl/gl-93h-toc.htm
c) M.G.L., Ch 93I, available at www.mass.gov/legis/laws/mgl/gl-93i-toc.htm
d) M.G.L., Ch 66A, Fair Information Practices Act, available at www.mass.gov/legis/laws/mgl/gl-66a-toc.htm
e) HIPAA Security Rule, available at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf
f) P.L. 107-204 (Sarbanes-Oxley Act of 2002), available at http://corporate.findlaw.com/industry/corporate/docs/publ107.204.html and www.soxlaw.com/
g) Federal Information Security Management Act of 2002 (FISMA), available at http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
h) Federal Information Systems Control Audit Manual (FISCAM), available at http://www.gao.gov/products/GAO-09-232G
i) National Institute of Standards and Technology (NIST) Special Publications (800 series), available at http://csrc.nist.gov/publications/PubsSPs.html.

Documents that contain more detailed procedures supporting CommCorp's Information Security Policy include:
Commonwealth Corporation Information Security Manual, available at *U:\Information Security*

**VII. OWNERSHIP and APPROVAL**

The Information Security Officer (ISO) is the owner of this document and is responsible for ensuring that this procedure is reviewed, continuously maintained and enforced within the agency. The President is responsible for approving the contents of this document, and the ISO and President are responsible for self-certifying its enforcement.

**VIII. DOCUMENT HISTORY**

| Date | Action/Version | Effective Date | Next Review Date |
|---|---|---|---|
| 09/17/2009 | CommCorp Information Security Policy, Draft | 09/17/2009 | Ongoing |
| 01/22/2010 | CommCorp Information Security Policy, Draft 2 approved by the Information Security Task Force | 01/22/2010 | |
| 02/26/2010 | CommCorp Information Security Policy finalized | 3/1/2010 | |

**IX. SIGNATURES**

**The document was approved by the authorized ISO on the date indicated, and is issued on a version controlled bases under his/her authority as signed below.**

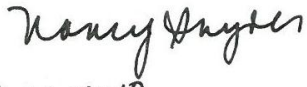
**Name:** NAVJEET SINGH

**Signature:** 

**Date:** 2/26/2010

**The document was approved by the President of Commonwealth Corporation on the date indicated, and is issued on a version controlled bases under his/her authority as signed below.**

**Name:** Nancy Snyder

**Signature:** 

**Date:** 2-26-2010

**APPENDIX A**

# Acknowledgement of Commonwealth Corporation's Information Security Policy

Period Covered: March 1, 2010 – June 30, 2011

I, _____(employee name), hereby acknowledge by my signature below, that I have read Commonwealth Corporation's Information Security Policy, that I have received training concerning the policy, and that I understand and will comply with the terms of this policy.

_____

Signature

_____

Date

**An executed copy of this Acknowledgement will be kept in each employee's personnel file, in the possession of CommCorp's Human Resources Manager.**

**APPENDIX B**

**COMMONWEALTH CORPORATION**

**INFORMATION SECURITY INCIDENT REPORT FORM**

<table>
<tr><td colspan="3">Note: Any agency staff member can submit this incident report form.</td></tr>
<tr><td colspan="2">Report # (completed by agency ISO or designee): _____</td><td>Date of Report:</td></tr>
<tr><td colspan="2">Name and title of person reporting this incident:</td><td>Agency/Location:</td></tr>
<tr><td colspan="2">Name of Agency Information Security Officer (ISO):</td><td>Agency/Location:</td></tr>
<tr><td colspan="3">Assets Affected: (what services, facilities or equipment were breached?)</td></tr>
<tr><td>Date/Time incident was observed:</td><td colspan="2">Who Observed the incident?</td></tr>
<tr><td colspan="3">Description of weakness or incident: (replace this text with: what malfunctioned? what actions were being executing? what things or strange behavior occurred, what appeared to be the breach or other issue? what breaches of physical security did you see?)</td></tr>
<tr><td>Person Submitting this Report</td><td>Signature:<br>_____</td><td>Date Signed:<br>_____</td></tr>
</table>

| **Incident assessment (completed by agency ISO or designee)** | | |
|---|---|---|
| **Initial Analysis** *(circle one)* | Incident Vulnerability Reportable Incident Unknown | |
| Comments: | | |
| **Final Analysis** *(circle one)* | Incident Vulnerability Reportable Incident Unknown | |
| Comments OR Corrective Action: | | |
| **Reporting determination:** | ☐ President and General Counsel of Commonwealth Corporation<br><br>After consultation with President and General Counsel a determination will be made to report the incident to the Board of Commonwealth Corporation, The Attorney General, The Director of Consumer Affairs and Business Regulation and the residents whose information may have been affected. | |
| **Name:**<br><br>_____ | **Signature:**<br><br>_____ | **Date Signed:**<br><br>_____ |

**APPENDIX C**

## Commonwealth Corporation Grantee or Contractor Certification of Compliance with Commonwealth Corporation's Information Security Policy

**Background.** Funds awarded by Commonwealth Corporation (CommCorp) through the attached grant agreement may represent funds derived from an executive agency of the Commonwealth of Massachusetts. Grantees and sub-grantees may be required, as a condition of the program being funded, to collect, process, access, communicate, report, or manage personal data of clients, customers, applicants or participants. Grantee(s) are required to certify that they understand the requirements of CommCorp's Information Security Policy, and further certify that they will protect the privacy and security of any and all personal information to the standard established in EO 504 and the policies of CommCorp. CommCorp's Information Security Policy (which includes links to relevant state regulations and policies, including EO 504) is available at: http://commcorp.org/InformationSecurityPolicy.html

**Certification.** Grantee shall, in connection with its performance under this grant agreement:

(a) obtain, read, review and comply with CommCorp's Information Security Program (CC-ISP) and any pertinent security guidelines, standards and policies; and comply with all of the Security Policies issued by the Commonwealth of Massachusetts Information Technology Division (ITD Policies);

(b) communicates to and ensures compliance by all grantees employees, contractors, sub-grantees and subcontractors the standards of practice and expectations contained in both the CC-ISP and ITD Policies;

(c) implement and maintain all reasonable and appropriate security procedures and practices necessary to protect personal information related to clients, customers, applicants or participants that is in the grantee's possession from unauthorized access, destruction, use, modification, disclosure, or loss;

(d) be responsible for the full or partial breach of any of these terms by its employees, contractors, or subcontractors during and after the term of this grant agreement;

(e) in the event of any unauthorized access, destruction, use, modification, disclosure, or loss of personal information, to (i) immediately notify CommCorp if the grantee becomes aware of such unauthorized use; (ii) provide full cooperation and access to information necessary for CommCorp to determine the scope of the unauthorized use; and (iii) provide full cooperation and access to information necessary for CommCorp and grantee to notify individuals whose personal information was the subject of such unauthorized use.

The breach of any of these terms may be regarded by CommCorp as a material breach of this grant agreement, such that CommCorp may exercise any and all right and remedies, including without limitation, indemnification, withholding of payments, contract suspension, or termination.

| | |
|---|---|
| Signature of Authorized Representative | Name and Title of Signatory |
| Grantee Organization Date | |