ACCEPTABLE USE POLICY

Document Classification:

Controlled

Version Number: 1.8

Issue Date: March 23, 2020

Table of Contents

1. POLICY STRUCTURE AND DEFINITIONS

1.1 POLICY STRUCTURE

This policy document contains the following elements:

- **Purpose**: This section clearly states the purpose of the policy with regards to acceptable use of NCDC assets.
- **Scope**: This section defines various internal and external entities as well as the people to which a particular policy statement applies.
- **Policy**: This section describes the policy statements of acceptable use of NCDC assets
- **Related NCDC Documents**: This section mentions other NCDC documents, which can be referred to along with this policy document.
- **Compliance**: This section contains a statement that NCDC policies will be complied with and that violations may result in disciplinary action.
- **Waiver Criteria**: This section provides a formal process for obtaining approval for a waiver to the policy. Waivers will only be approved in exceptional situations when communicating non-compliance with the policy for a specific period of time.
- **Executor(s):** The person / people responsible for implementation of this policy.
- **ISO27001:2013 Control References**: This section provides references to security controls that have been used here in this policy.

1.2 DEFINITIONS

The terms used in this document shall have the meanings as defined in the NCDC Glossary which can be found at http://www.ncdc.gov.sa.

2. PURPOSE

The purpose of this policy is to outline the acceptable use of NCDC assets that include personal computers, servers, networks, applications and data stored in systems. This Policy is intended to protect the employees and NCDC. Inappropriate use exposes NCDC to risks including virus attacks, compromise of network systems and services, and legal issues.

3. SCOPE

The scope of this policy applies to NCDC employees, contractors or any other workers ("users") who will use NCDC assets.

4. POLICY

4.1 GENERAL TERMS

- Users shall use NCDC assets only for the authorized purposes.
- Users shall sign NCDC Acceptable Use Agreement before using NCDC systems/services.

4.2 COMPUTER USAGE

- Users shall have regular backup for the data stored on their computer machine.
- Users shall log-off the computer machine when away from desk to prevent unauthorized access to his computer.
- Users shall be responsible for the security of their passwords and accounts by keeping it confidential and not sharing them with others. [Refer to NCDC Access Control Policy]
- For security and network maintenance purposes, authorized individuals may monitor equipment, systems and network traffic at any time.
- Users shall practice Due Care to protect and maintain NCDC assets stored on portable devices from loss, theft and damage.
- Making administrative or hardware changes to NCDC systems is governed by NCDC Change Management Policy.[Refer to NCDC Change Management Policy]
- Users shall not delete copy or modify files that belong to other users without permission.
- Users shall not conduct port scanning, security scanning or executing any form of network monitoring unless this activity is part of the user's normal duty.

4.3 SOFTWARE USAGE

- Third party copyrighted information, software or other copyrighted source, that NCDC does not have specific approval or license to store and/or use, shall not be stored on the systems that owned by or used for NCDC work.
- Users shall not install or use hardware or software tools that could be employed to evaluate or compromise system security unless this activity is part of the employee's normal duty.

- Users shall not copy software provided by NCDC to any storage media, transfer such software to another computer, or disclose such software to outside parties without permission from NCDC Management.

4.4 ELECTRONIC IDENTITY

- Users shall protect private keys and tokens to prevent loss, disclosure, modification and use by other persons.
- Users shall notify the CSP immediately if private keys have or may have been compromised or tokens are lost/damaged in anyway.
- Accessing to computers or devices containing the private key shall be controlled.
- Users shall protect their passwords/PINs that used to access private keys.
- Users shall comply with the terms and conditions regarding the issuance of certificate as prescribed in the Government CA Certificate Policy (CP) published at http://www.ncdc.gov.sa

4.5 EMAIL USAGE

- Users shall utilize NCDC email system for business activities only.
- If an e-mail message contains potentially important reference information or has a value to NCDC business, it must be retained for future reference.
- Any confidential or controlled information transmitted over an email message shall be encrypted.
- Because of mailbox size limitation, users shall move important emails to a secure storage area and ensure regular back up is maintained.
- Users must use extreme caution when opening email attachment from unknown sources, which may contain viruses.
- Users shall not send harassing or offensive email to others through NCDC email account.
- Users shall not forward attachments containing suspicious viruses or malicious code threats. On the contrary they should immediately delete them and report the incident to the IT helpdesk.

4.6 INTERNET USAGE

- Users shall not use any external sources of Internet connection other than the connection provided by NCDC.
- Users shall be careful when downloading files form internet that may contain malicious software.
- The installation of software such as Instant messaging technologies, without business needs, is prohibited.
- Users shall not access sites that impinging on public order, religious values and public morals.

5. RELATED NCDC DOCUMENT

- NCDC Acceptable Use Agreement
- Government CSP Subscriber Request Form
- Government-CA Certificate Policy
- NCDC Access Control Policy
- NCDC Change Management Policy
- NCDC Information systems, Acquisition, Development and Maintenance Policy

6. COMPLIANCE

Compliance with this policy is mandatory and will be reviewed periodically by Trust Services Governance General Department. Violations of NCDC policies, standards, and procedures will result in corrective action by NCDC management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets.
- Other actions as deemed appropriate by NCDC management, Business Support department , and Trust Services Governance General Department.

7. WAIVER CRITERIA

Requested waivers must be formally submitted to NCDC, including justification and benefits attributed to the waiver, and must be approved by NCDC Management. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time (subject to a maximum period of 1 year). At the completion of the time period the need for the waiver should be reassessed and re-approved, if necessary. No policy should be provided waiver for more than three consecutive terms. The waiver should be monitored to ensure its concurrence with the specified period of time and exception. All exceptions to this policy must be communicated through the Policy Waiver Request Form.

8. EXECUTOR

The following are the executor of this policy:

- Business Support department
- NCDC Employees/Contractors

9. ISO27001:2013 CONTROL REFERENCES

- A.8.1.3 Acceptable use of assets