Policy Guidelines

for

Handling Audit related Data

Version 1.0

1. Preamble

In the light of the growth of IT sector in the country, it is the compelling need to build trust in the IT assets & information resources handling critical information resulting into security of information more important than ever before. Ever increasing number of gaps in the information security measures, network & systems vulnerabilities and hacking incidents have heightened the concerns with regard to security of sensitive information. These gaps can be identified and addressed by auditing level of information security of an organization periodically through validation of information security risks, mitigation measures, controls, policies and procedures in the organization & comparison with the industry best practices. The auditors, during and after the audit assignments have access to customer sensitive information and may result in leakage of information in case proper policies and processes are not in place.

In order to assist the auditors in having appropriate policies and processes for secure handling of audit related data, an attempt has been made to provide policy guidelines, as a means of assurance to the auditee as well as other stakeholders concerned. This policy is applicable to auditors who are empanelled by CERT-In and also to those who were empanelled but their empanelment could not continue after certain period. This will also provide guidance to the auditee organisation regarding collection, preservation, sharing & disposal of data by the auditor before entering into the contract with auditee.

2. Definitions

The term, “Auditor” shall include any organization empanelled(current & past) by CERT-In for auditing, including vulnerability assessment and penetration testing of computer systems, networks, computer resources & applications of various agencies or departments of the Government, critical infrastructure organizations and those in other sectors of Indian economy.

The term, “Auditee” shall include the directors, officers, employees, agents, consultants, contractors and representatives of Auditee, including its affiliates and subsidiary companies. Auditee is an organization who enters into contract with the auditor for carrying out its information security audit.

3. Purpose

The purpose of this document is to provide guidance on:

3.1. Mechanism followed for handling, storage, accessing, retention and destroying Auditee related data.

3.2. Recommended ways for disclosure & sharing of data within and outside the auditor organization including data sharing with the overseas partners/entities.

3.3. Secure communication with the auditee organization regarding the audit outcome and related matters.

3.4. Handling of the incidents where client audit related data is leaked (intentionally or unintentionally).

3.5. Key issues regarding Non-disclosure Agreement (NDA)

4. Scope

This policy is applicable to:

4.1. All CERT-In empanelled Auditors (current and past)

4.2. All employees, contractors and third party personnel having access to auditee related data obtained as a result of engagement by auditor.

5. Policy Statements

5.1. Mechanism followed for handling, storage, accessing, retention and destroying client data

5.1.1. The security and confidentiality of the auditee related data should be managed effectively. Processes and procedures should be defined and documented to handle auditee related data during and after the audit.

5.1.2. Devices such as Desktops/Laptops/Tablets/Mobiles/Pen Drives etc. used for conducting the audit should have sufficient security measures implemented , as may be necessary, including use of encryption to prevent data leakage and device theft.

5.1.3. Access to auditee related data should be controlled using appropriate access control mechanisms and the data access should be only on need to know basis.

5.1.4. Project documentation to be archived on an access controlled storage preferably in an encrypted form and should be permanently deleted from the desktop/laptop or other temporary storages (used during the course of audit) after the project completion.

5.1.5. Auditee related data should only be retained for specific period of time as in agreement with the auditee and disposed-off as per defined & agreed process.

The collection, preservation and disposal of data collected by the auditor should be in accordance with the agreement entered between Auditor & Auditee. In any case, the auditor will not leak data at any time (during or after the audit) to any third party without the permission of Auditee.

5.1.6. Auditee related data should be stored only on systems located in India with adequate safeguards and should keep the auditee informed of the means & location of storage and seek auditee's consent where necessary.

5.2. Recommended ways for disclosure & sharing of data within and outside the auditor organization including data sharing with the overseas partners/entities

5.2.1. The sharing and disclosure of auditee related data, where necessary, should only be done with prior consent of auditee organization.

5.2.2. The auditee/project related data should not be shared with or disclosed to any overseas partner, unless specifically authorized by the auditee.

5.3. Secure communication with the auditee organization regarding the audit outcome and related matters.

5.3.1. The audit outcome & related matters should only be communicated to the specified Point of Contact (POC) of the auditee organization.

5.3.2. The audit report should only be shared using secure methods such as use of passwords, encryption etc.

5.3.3. Audit report should not be shared / hosted on online internet file services, online sharing platforms and cloud services, unless the service is under technical and administrative control of the auditing organization or as specifically authorized by the auditee.

5.4. Handling of the incidents where client audit related data is leaked (intentionally or unintentionally)

5.4.1. Organization should have Incident Management Policy and related processes in place with clearly defined escalation matrix and procedures to deal with non-compliance. This process for dealing with incidents should be shared with the auditee.

5.4.2. The auditing organization should inform the auditee of any incident related to the project/auditee related data and take all necessary actions to address the

incident as may be required.

5.4.3. The auditing organization should work jointly with the auditee to minimize impact due to data loss and support him in taking suitable measures.

5.5. Key issues regarding Non-Disclosure Agreement (NDA)

5.5.1. The auditing organization should have signed NDA in place with their employees.

5.5.2. NDA with auditee organization must be signed before commencement of the project & should be legally enforceable. CERT-In Model NDA, as published on CERT-In's website, may be used /customized as per project/organization requirement.

5.5.3. The auditing organization as well as its employees and contractors should be aware of the consequences of non-compliance with NDA & related liabilities.