IRD-Institute for Rural Development, Vijayapur

Annexure-30

Assets Management Policy

1. Purpose

The purpose of the Asset Management Policy is to establish the rules for the control of hardware, software, applications, and information used by.

2. Audience

The Asset Management Policy applies to individuals who are responsible for the use, purchase, implementation, management, and/or maintenance of information resources in the organization.

3. Contents

Hardware, Software, Applications, Data, Mobile Devices, Media Destruction & Re-Use, Backup, Removable Media and all movable assets of the organization.

4. Policy

Hardware, Software, Applications, and Data

- All hardware, software, and applications must be approved, inventoried, and purchased by IT.
- Installation of new hardware or software, or modifications made to existing hardware or software, must follow approved procedures and change control processes.
- All purchases must follow the defined Purchasing Process.
- Software used by employees, contractors, and/or other approved third parties working on behalf of must be properly licensed.
- Software installed on computing equipment, outside of that noted in the Standard Software List, must be approved by Organization management.
- Only authorized cloud computing applications may be used for sharing, storing, and transferring confidential or internal information.
- The use of cloud computing applications must be done in compliance with all laws and regulations concerning the information involved, e.g., personally identifiable information, protected health information, corporate financial data, etc.
- Two-factor authentication is required for external cloud computing applications with access to any confidential information for which has a custodial responsibility unless a waiver/exception form is formally approved.
- Contracts with cloud computing application providers must address data retention, destruction, data ownership, and data custodian rights regarding stored data.

Dr. BABU. G. SAJJAN.
B.A.,LL.B.(Spl.),MA(S.W),Ph.D
Chief Executive Officer,
Institute for Rural Development
VIJAYAPUR.

- Hardware, software, and application inventories must be maintained continually and reconciled no less than annually.
- A general inventory of information (data) must be mapped and maintained on an ongoing basis.
- All assets must be formally classified with ownership assigned.
- Maintenance and repair of organizational assets must be performed and logged in a timely manner and managed by Organization management.
- Company assets exceeding a set value, as determined by company, are not permitted to be removed from Company's physical premises without management approval.
- If a Company asset is being taken to a "High-Risk Area", as defined by the FBI and Office of Foreign Asset Control, it must be inspected and approved by IT before being taken offsite and before reconnecting to the Company network.

5. Mobile Devices

- Company does not allow **personally-owned mobile devices** to connect to the Company corporate internal network.

OR

- The use of a **personally owned mobile devices to** connect to the Company network is a privilege granted to employees only upon formal approval of IT management.
- **Mobile devices** used to connect to the Company network are required to use the approved **Mobile Device Management (MDM)** or **Mobile Application Management (MAM)** solution, defined by IT management.
- **Mobile devices** that access Company email must have a PIN or other authentication mechanism enabled and in accordance with the Authentication Standard.
- **Confidential data** should only be stored on devices that are encrypted in compliance with the Company Encryption Standard.
- All **mobile devices** with access to (Company) data should maintain up-to-date versions of all operating systems and applications.

6. **Media Destruction & Reuse**

- Media that may contain **confidential** or **internal information** must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Media reuse and destruction practices must be conducted in compliance with Company's Media Reuse and Destruction Standards.
- All decommissioned media must be stored in a secure area prior to destruction.
- Media reuse and destruction practices must be tracked and documented.
- All information must be destroyed when no longer needed, included encrypted media.

Dr. BABU. G. SAJJAN.
B.A.,LL.B.(Spl.),MA(S.W),Ph.D
Chief Executive Officer,
Institute for Rural Development
VIJAYAPUR.

7. Backups

- The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the information owner.
- The Company backup and recovery process for each system must be documented and periodically reviewed according to the defined review schedule, approved by (Company) leadership.
- The vendor(s) providing offsite backup storage for Company must be formally approved by (Company) leadership to handle the highest classification level of information stored.
- Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems. Additionally, backup media must be protected in accordance with the highest Company sensitivity level of information stored.
- A process must be implemented to verify the success of the Company electronic information backup.
- Backups must be periodically tested to ensure that they are recoverable in accordance with the backup standard.
- Multiple copies of valuable data should be stored on separate media to further reduce the risk of data damage or loss.
- Procedures between Company and the offsite backup storage vendor(s) must be reviewed at least annually and then approved by IT management or (Company) leadership.
- Backups containing **confidential information** must be encrypted in accordance with the Encryption Standard.
- **Signature cards** held by the offsite backup storage vendor(s) for access to Company backup media must be reviewed annually or when an authorized individual leaves Company.
- Backup tapes must have at a minimum the following identifying criteria that can be readily identified by labels and/or a bar-coding system:
    - System Name
    - Creation Date
    - Sensitivity Classification
    - Company Contact Information

8. Removable Media

- The use of **removable media** for storage of Company information must be supported by a reasonable business case.

Dr. BABU. G. SAJJAN.
B.A.,LL.B.(Spl.),MA(S.W),Ph.D
Chief Executive Officer,
Institute for Rural Development
VIJAYAPUR.

- All **removable media** must be approved and inventoried by Company IT or leadership prior to use.
- **Personally owned removable media** use is not permitted for storage of Company information.
- Users are not permitted to connect **removable media** from an unknown origin.
- **Confidential and internal** Company **information** must not be stored on **removable media** without the use of encryption.
- The loss or theft of a **removable media** device that may have contained any Company information, regardless of sensitivity, must be reported to Company IT management.
- Company will maintain inventory logs of all media and conduct media inventory audits at least annually.
- The transfer of information to removable media will be monitored.

9. Waivers

Waivers from certain policy provisions may be sought following the Company Waiver Process.

10. Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Chief Executive Officer

IRD Vijaypur
Dr. BABU. G. SAJJAN.
B.A.,LL.B.(Spl.),MA(S.W),Ph.D
Chief Executive Officer,
Institute for Rural Development
VIJAYAPUR