Writer Corporation

Data Protection Policy

1. Introduction

The Data Protection Policy (DPP) lays a solid foundation for the development and implementation of secure practices within Writer Corporation (the Company). The policy parameters are themselves not instructional or overly descriptive. They represent the rules to be adhered to by the organization. Compliance to the policies can be ensured by thorough understanding and adherence to the corresponding procedures outlined as Standard Operating Procedures (SOP).

This DPP provides a robust security framework of “Confidentiality” “Integrity” and “Availability” encompassing of Risks, threats, vulnerabilities and impacts.

It is the responsibility of every employee and outsider working with Writer Corporation to protect the information assets with which they are entrusted with; from a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, espionage, privacy violation, service interruption, and natural disaster.

The information being a critical asset needs to be protected at all stages of its life-cycle from the moment it is created or received through processing, communication, transportation, storage and dissemination to others.

1.1 Objective

The security of the Information Technology (IT) assets of Writer Corporation such as office supplies / equipment, information resources, computer systems, network resources is vital to its business. Effective and efficient security procedures are to be followed within the company’s facilities and in its operations, to ensure information and resources are available only to users who have access to it and restricted to others.

1.2 Scope

This IT general controls and security policies are applicable to the following

- All facilities and offices at all locations of Writer Corporation
- Employees, contractors, consultants, temporaries and other workers at Writer Corporation, including all personnel affiliated with third parties#. Third parties are referenced as - Contract staff, Vendors onsite, Consultants onsite, Customers onsite; at Writer premises and network.
- Subcontractors - Selective elements of this policy will be applicable to Subcontractors as well and commitment for adherence to the same need to be ensured in the agreement signed with the Vendor of Writer Corporation..
- Writer owned equipments, assets and applications *

2. Acceptable Use Policy

2.1.1 Security and Proprietary Information

a) Sharing of login names and passwords are not allowed.

b) Postings by employees from a Writer Corporation email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Writer Corporation , unless posting is in the course of business duties.

c) Internet / Intranet / Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Writer Corporation. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

2.1.2 Unacceptable Use

The following activities are strictly prohibited, with no exceptions:

a) Under no circumstances an employee of Writer Corporation is authorized to engage in any activity that is illegal under law while utilizing Writer Corporation - owned resources.

b) No user is allowed to download and install applications / files without proper licensing.

c) Introduction of malicious programs into the network or server by a user (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

d) Circumventing user authentication or security of any host, network or account.

Writer Corporation will institute a process of granting access to information resources on the basis of “least privilege” and “need to know/ need to do” to users. Writer Corporation will put in place operational and monitoring mechanisms to achieve logical access control. The IT department will be responsible for providing all legitimate users access rights and privileges for information resources, after receipt of proper authorization.

Any change in the job profile leading to change in the user access needs to be intimated to respective business / corporate IT by business / Corporate HR.

2.1.3 Review of Access Rights

a) Access rights for each application user will be reviewed annually by the business head with support from respective application team lead from IT. Changes / additions / deletions to user access will be implemented by IT. This will be a part of annual recertification process.

2.1.4 Deactivation of users and disabling inactive user accounts

a) Based on the Employment Settlement / Relieving / Clearance Form from HR, all the necessary network related ID’s (email, network login etc) will be deactivated after the relieving date of the employee.

2.1.5 Storage Media

a) USB devices: To prevent unauthorized transfer of information through USB Storage ports, these ports will be disabled. Any user requiring access to USB ports must get an authorization from the respective SBU CEO/Functional Head as per the approval hierarchy matrix.

3. Password Management

3.1.1 Base level Standards

User level Passwords:

a) All user-level passwords (e.g., email, desktop computer, etc.) must be changed every 60 days. No user accounts will have system-level privileges granted. Each user will have a single user id. A user id may have multiple sign-on enabled. In case of any exceptions due to functional requirement approval matrix as mentioned in section 23 should be followed.

3.1.2 Password Creation standards

IT policy mandates use of strong passwords with following standards.

- 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, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.

NOTE: These things are forced via central Active Directory.

3.1.3 Account Lock-out

a) If a user attempting to log into a system, enters the wrong "User Id" or "password" for 3 times, that user's account will be locked automatically.

4. Virus Protection

a) The antivirus system will be installed and configured centrally by IT team. However The primary user of a computer system is responsible for keeping the computer system compliant with this Anti - Virus protection policy and should not block / suppress system initiated antivirus scans.

b) Freeware or shareware is not permitted, these freeware or shareware on disk or downloaded from a bulletin board or website is one of the most common infection sources.

c) An unfiltered virus constitutes a security incident and must be reported. A user that detects such a virus needs to notify the IT facilities.

d) All desktops, laptops and servers will have scheduled virus scans. No users should disable the scheduled virus scanning and auto-updates.

e) To enable data to be recovered in the event of virus outbreak regular backups should be taken by users. Users who want their data backed up will have to store their files on designated storage devices / shared networks.

5. Internet Usage

5.1.1 Restriction on Internet Access

Other activities that are strictly prohibited include, but are not limited to:

a) Misusing, disclosing without proper authorization, or altering customer or personnel information.
b) Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations Indian laws and regulations.
c) Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
d) Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
e) Any form of gambling and playing online games.
f) Unauthorized downloading of any pirated software, shareware programs or files for use without authorization in advance from the IT Department and the user’s manager.
g) Usage in any form that violates any Indian government or Writer Corporation rules, regulations or policies.
h) Hosting of personal web sites using company’s assets.
a) The data card will be subject to a monthly usage limit prescribed from time to time
b) Data card users should adhere to Internet usage policy and email policy at all times.

5.1.2 Email on Blackberry Policy

a) Email will only be provided on company owned Blackberry handsets / devices based on the approval from their respective Business CEO / Corporate Function Head.
b) In case of business requirement, email will be configured on personal devices with the prior approval of Business CEO / Corporate Function Head.
c) When the person leaves the organisation, address book contact details and emails will be deleted as per employee separation process.

6. Physical Security of IT assets

6.1.1 Entry in to Restricted Areas

a) Entry into areas housing sensitive IT resources such as data centre / Server rooms is restricted, and should be monitored and logged.
b) The CIO/ National Manager IT Infrastructure will authorize request for access.

6.1.2 Managing Network Devices

a) LAN equipment, switches, routers in tier-1 cities will be kept in secure networking rooms /lockable enclosures.
b) Hub rooms will be kept locked at all times. Access to hub rooms will be restricted to IT Services staff only.
c) In tier-2 and tier-3 cities safeguarding of IT assets is the responsibility of local admin department.

6.1.3 Managing Unattended Workstations

a) Users must logout of their workstations when leaving from office.
b) Users must lock their workstation when leaving it unattended for more than 10 minutes.
c) All unused workstations including monitors must be switched off outside working hours.

6.1.4 Managing Servers

a) Accessibility to servers is restricted to a limited number of authorized personnel, and passwords are selected based on strict rules. For additional security, all servers must be located in a secured environment.
   - Server room will be restricted to authorised IT Facilities Management (FM) staff only
   - Access to the system console and server disk/tape drives will be restricted to authorised IT facilities staff only

6.1.5 Electrical Security

a) All servers, switches, routers and other critical network equipment should be on power supplied by UPS
b) In the event of a mains power failure, the UPS's should have sufficient backup to keep the network and servers running for at least a half-an-hour.
c) Local Admin has the accountability to ensure spike free electrical supply to IT equipment.

6.1.6 Movement of Hardware

a) In case of computer hardware being sent out of Writer Corporation offices for repairs or to other branches or for maintenance work, gate pass / challan will be prepared by the IT engineer. The gate pass has to be approved by the Branch head / Reporting Manager and IT Client Services Operations Manager. Administration department will maintain a central log / file of the gate passes / challans.
b) Prior to moving it out, a complete analysis of data residing on the computer hardware (if any) should be carried out by the user.
c) The concerned data owner(s) should analyse the data and depending upon the classification of the data, appropriate security procedures should be followed before sending the hardware out. This may include removing the data from the hardware going out for repairs and backing it up in other systems and dispatch the hardware without any live data.

7. Disposal or Re-Use of Equipment

- In order to protect our data, all storage mediums must be properly erased before being disposed of.
- Laptops / Desktops should be formatted before disposal or reuse.
- Rental machine should be formatted before putting on Writer network. These rental machines should be formatted before returning them to the supplier.