Acceptable Usage policy for end users

DOCUMENT SUMMARY:

AUTHOR	ARUL ARCHANA A	
REVIEWED BY	JAGANNATHAN N	
CURRENT VERSION	1.1	
DATE OF CURRENT VERSION	04-06-2024	
DATE OF ORIGINAL VERSION	16-08-2023	
DOCUMENT NAME	A-5.10-Acceptable Usage policy	
DOCUMENT TYPE	Acceptable Usage policy	
DOCUMENT CIRCULATION	ALL TEAMS	
OWNER	CISO	
APPROVED BY	NAME:	SARAVANA KUMAR S
	DESIGNATION	CHIEF INFORMATION SECURITY OFFICER

REVISION HISTORY

Version	Revision	Issue Date	Changes
1.0		16-08-2023	First Draft
1.0	1	04-06-2024	In Document summary, Owner changed from MANAGER SECURITY OPERATIONS to CISO and Designation changed from MANAGER SECURITY OPERATIONS to CHIEF INFORMATION SECURITY OFFICER

Table of Contents

1.0 Introduction

This policy addresses the intent of Fourth Dimension Technologies Pvt Ltd. (Hereinafter referred to as 4D), to safeguard computing resources from Internet and email-based threats. This policy shall underline appropriate user etiquette for workstation, Internet and email usage and define procedures for safeguards from Internet and email borne threats.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment, software, operating systems, storage media, and network accounts providing electronic mail, www browsing, and FTP, which are the property of 4D. These systems are to be used for business purposes in serving the interests of the 4D, and of their clients and customers in the course of normal operations. These rules are in place to protect the interest of 4D and its employees. Effective security is a team effort involving the participation and support of every 4D employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

3.0 Workstations Security Policy

Use of Laptop

Employees are responsible for the security and integrity of information stored on personal laptop. Users should be aware that the data they create on the corporate systems remains the property of 4D. User responsibility includes regularly saving work onto the shared network drive/OneDrive. All the process related business data should be kept in the assigned process folders, thereby enabling the System Admin to take backup of these critical business data.

Personal Work

Computing facilities, services, and networks may not be used for work other than that of 4D.

Resources Sharing

There should not be any shared folder created on the local laptop provided to individual users. Users shall not create any shared folder in their respective laptop. Data on the network shares are secured using Windows/OneDrive permissions and access level controls. All directories and sub-directories, which are shared, shall be protected by proper user authentication and permissions to access with relevant access rights.

Avoid storing passwords or other information that can be used to gain access to other network resources. Computer accounts, passwords, and other types of authorization are assigned to individual Employees who are responsible for its security. Revealing user account password to others or allowing use of user account by others is strictly prohibited. This includes family and other household members when work is being done at home.

Use of privileged access

Special access to information or other special computing privileges is to be used during official duty only. Information that is available through special privileges is to be treated as private & confidential. A deliberate attempt to degrade the performance of a computer system or network or access to any restricted IT Infrastructure is prohibited.

Restriction on the Use of Privilege Account

- Personnel using the organizations resources are prohibited from gaining unauthorized access to any other information system or in any way damaging, altering the information, or disrupting the operations of the systems thus accessed.
- Personnel are prohibited from capturing or otherwise obtaining passwords, encryption keys or any other access control mechanism which could permit unauthorized access.
- Personnel should not attempt to compromise the internal controls, security, resources etc., unless specifically approved and record of the same should be maintained. E.g. for test etc...
- User should not exploit vulnerabilities or deficiencies in IT security systems to damage system or information, to get hold of resources beyond what they are authorized to, to gain access to other systems for which they do not have authorization, or to take away resources from other users. Such vulnerabilities / deficiencies should be reported to appropriate authority as per incident handling mechanism of the organization.
- Non-production staff such as internal auditors, programmers, security administrators, etc. should not be permitted to update the production / live data, unless authorized.
- The use of direct access to data is not permitted unless specifically permitted by appropriate authority to authorized person.
- Changes to privileged accounts should be logged for periodical review.

Software Copyright and Licenses

4D shall procure Software licenses to be used in 4D for facilitating its operations. The same needs to be evaluated and approved by Information Security Steering Committee for procurement and use in 4D.

Unacceptable Usage activities

- The harmful activities such as creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to equipment, software, applications, data belonging to 4D or clients; and the like are strictly prohibited.
- Port scanning or security scanning is expressly prohibited unless prior notification to Information Security Steering Committee.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty, is prohibited.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack) and providing information about, or lists of, 4D employees to parties outside 4D, are prohibited.
- Security breaches or disruptions of network communication, include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties, is prohibited. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Using 4D computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited.
- Leaving confidential or sensitive information on printing facilities, photocopiers, and facsimile machines.

Unauthorized access

4D employees shall not:

- Damage computer systems
- Obtain extra resources which are not authorized to an individual
- Deprive another user of authorized resources.
- Gain unauthorized access to systems.

By using knowledge of:

- A special password.
- Vulnerabilities in computer systems
- Another 4D user’s password
- Accessibility of a 4D user during a previous position or role

4.0 Laptop Security Policy

Physical Security

The physical security of the laptop is the responsibility of the user to whom the laptop is provided.

The following precautions to be ensured

- Operating System password to be enabled as per the password policy ie
  - a) Use a mixture of upper case and lower case letters, numerals and special characters, if possible
  - b) Use at least 8 characters, or the maximum number of characters.
  - c) Do not reuse old passwords.
  - d) Do not use trivial passwords (e.g. words from dictionaries, keyboard patterns, user IDs).
- Clear screen policy to be invariably followed.
- While travelling the user shall ensure that the bag containing laptop is physically secured under lock and key.
- While travelling via flight the user shall carry the laptop as personal baggage.
- While using the laptop at external locations cable lock shall be used to secure the laptop.

Laptop Data backup policy:

Data on the laptop is more expensive to replace than the hardware. The following must be followed:

- Users are requested to store the data in OneDrive so that the data will be available wherever required.
- All the data should be classified by sensitivity (ie., Restricted, Private, or Internal, Public) in Header.
- Anti-Virus should always be updated immediately after the return of the user.
- The user should access the company’s network only after updating the anti-virus.

User role

- User will be responsible for any accidental damage due to tea, water, or other factors.

- In case of loss or theft of Laptop the cost of the laptop will be recovered from the employee per the terms of this policy. In case of loss, the employee may approach the ISSO.
- The primary responsibility to protect company asset given to the employee for use, lies with the employee.
- Only if ISSC finds that the employee has been diligent in his/her care and protection of the company property and that proper follow-up procedure to file the claim has been followed (e.g. lodging the FIR, submitting documents/copies of documents, etc.), then the cost of laptop replacement will be borne by the company. If the committee finds that the employee was negligent in his/her protection of the company asset, then it may call upon the employee to bear the full cost of the loss.
    - Laptop < 2 years old from the date of procurement – 100% of Laptop cost.
    - Laptop 2 to 3 years old from the date of Procurement – 50% of Laptop Cost
    - Laptop 3 to 4 years old from the date of procurement – 30% of Laptop Cost
    - Laptop 4 to 5 years old from the date of procurement – 20% of Laptop cost.

Do’s

- Usage is restricted to business purposes, and users must be aware of, and accept the terms and conditions of use, especially the responsibility of the security of information contained on the laptop, as well as the security of the laptop itself.
- Laptops should be kept out of sight and covered when stored in a vehicle.
- Laptops with unattended processes running on them must have some type of screen saver with password protection or keyboard locking program enabled on them.
- Laptops must be transported as carryon luggage when traveling by plane or bus, unless the carrier requires otherwise.
- Power on and system passwords should be used on laptops that are in highly accessible areas.
- Always scan files before accepting them onto the laptop. All downloaded files (includes internet, and e-mail) must be virus checked before saving to disk.
- All software used on the laptop must be licensed to an 4D and must comply with legal requirements and organizational standards
- Physical security and environmental security guidelines shall be followed for use of mobile device facilities outside the premises.
- Clear Desk and Clear Screen Policy shall be adopted while using the mobile device facilities.
- Keep all passwords pertaining to laptop access strictly confidential.
- Arrangements shall be made to ensure the availability of password in case of emergency.

- Automatic screen lock with password protection shall be used.

- The portable computers shall be protected against the malicious software as per the Antivirus Policy.

Don’ts

- Load software onto the portable computer at any time, and do not alter or delete the existing software or configuration options.
- Store songs, store official documents, unauthorized utilities, unauthorized software or other unauthorized materials on the laptop.
- Share laptop with anyone.
- Share passwords with anyone
- Write down any system boot up, e-mail and/or user account password.

Monitoring

All the data residing on the laptops is the property of the company. 4D reserves the right to install any monitoring software on the laptops and the right to monitor the company laptops for any inappropriate, abusive or unethical use. Employees who carry out any inappropriate, abusive or unethical use of the laptops can be held responsible and legal and / or punitive action will be taken up against them. All communications, including text and images, done using the laptops can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

5.0 Clear Desk and Clear Screen:

Employees are supposed to follow the following principles while operating in their workstations:

Clear Desk

- The working desk of the employees should be maintained neatly.
- The workspace should not have any extra things/ objects unattended. For e.g. important documents, files etc., which are not being used.
- Sensitive information on paper or electronic storage media should be locked away when not required or when the office is vacated.
- There should be no documents directly kept on the Desktop screen.
- Incoming and outgoing mail points to be protected and care should be taken to prevent access to mail by other persons.
- Documents of sensitive nature near printers, photo copier, scanner etc. should be immediately removed.
- Unauthorized use of photocopiers, scanners, digital camera etc. should be prevented.

Clear Screen

- 4D users shall either log off or lock the workstation if they will be away from their desk any length of time. (Shortcut combination- ⊞ + L- may be used.)

- The workstation shall be configured to lock automatically using a secure screen saver if it is not used for a period of 5 minutes.
- Unauthorized use of photocopiers, scanners, digital camera etc. should be prevented.

6.0 General Use and Security of Internet Activities

Use of Internet Restricted to Business Use Only

The Internet should be used as part of the normal execution of a user’s job responsibilities.

Representation of 4D Position

Internet connections should only be used for valid business purposes. As such, any information posted to discussion groups bearing the company address should only reflect the company positions. Information transferred from 4D should be in accordance with 4D Internet usage policy.

Discretionary viewing, downloading and/or transmitting materials (other than that required for business) that involve the use of obscene language, images, jokes, sexually explicit materials or messages that disparage any person, group or classification of individuals is strictly prohibited.

Internet E-mail Communications Considered Public

Any messages sent over the Internet are not considered secure unless additional measures are taken to protect such information (e.g., encryption). Users should communicate via e-mail as they would in a public place (e.g., if you are not comfortable saying something to a room of people, it should not be said via e-mail).

Internet Rules of Behavior

Using 4D facilities or equipment to make abusive, unethical or "inappropriate" use of the Internet will not be tolerated and may be considered grounds for disciplinary action, including termination of employment. Examples of inappropriate employee Internet use include, but are not limited to, the following:

- Conducting or participating in illegal activities, including gambling
- Accessing or downloading pornographic material
- Solicitations for any purpose which are not expressly approved by company management.
- Revealing or publicizing proprietary or confidential information
- Representing personal opinions as those of the company
- Making or posting indecent remarks

- Uploading or downloading commercial software in violation of its copyright
- Uploading or mailing of company's confidential documents without the permission/authorization of the concerned parties.
- Downloading any software or electronic files without reasonable virus protection measures in place
- Intentionally interfering with the normal operation of Internet gateway

Prohibitions on User Internet Activities

To prevent any appearance of inappropriate conduct on the Internet and to reduce risk to the organization, users should not:

- Enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of the company over the Internet
- Use the company logos or the company materials in any web page or Internet posting unless it has been approved, in advance, by the company management.
- Use software files, images, or other information downloaded from the Internet that has not been released for free public use.
- If a business need exists, then protective methods and software must be installed on the user's work-station to prevent hackers to get access to the data on the user's work-station
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company network or systems.
- Attempt to gain illegal access to remote systems on the Internet.
- Attempt to inappropriately telnet to or port scan remote systems on the Internet.
- Use or possess Internet scanning or security vulnerability assessment tools without the permission of the CISO.
- Post material in violation of copyright law
- Establish Internet or other external network connections that could allow other company users to gain access into 4D systems and information assets.

Unauthorized connections to Internet

Users of any computer that is attached to the 4D network should not be permitted to connect to Internet through unauthorized means of connectivity.

Restriction on Internet Transmission of Sensitive Company Information

Confidential information shall not be transmitted over Internet without reasonable security measures (such as encryption or other appropriate method) in place.

Restrictions on Internet Transmission of Sensitive Information

Credit card numbers, telephone calling card numbers, login usernames and passwords, and other parameters that can be used to gain access to systems or services should not be sent over the Internet in plain text.

Restrictions on Employee Production of WWW Pages

Employees are not allowed to produce web pages or sites that reference the company or affiliates, masquerade as the company, or in any way disclose any other information about the company without the written permission of the company management. Employees are not allowed to host personal sites on the company facilities.

Restrictions on Use of Internet for New Business channels

Users are prohibited from using new or existing Internet connections to establish new business channels, without the approval of the Managers. These channels include electronic data interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

Composition of Internet Passwords and User IDs

All Internet passwords and user IDs should meet 4D password standards as described in the Password Policy.

Virus Scanning of Downloaded Internet Information

All information downloaded to the company computing resources via the Internet should be screened with virus detection software prior to use. Refer to Antivirus Policy.

Restrictions on Posting Company Material to Anonymous FTP System

Users should not place the company material (software, internal memos, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar services, unless the Information Security officer has first approved the posting of these materials.

Internet usage Do’s and Don’ts

Do’s

- During upload/download of any files from the Internet, the users should ensure that these attachments are virus free and scanned by antivirus software.
- Download information only from secure sites as affirmed by the certificate availability.
- Read the security information relating to web pages during accessing web sites.
- All downloaded files must be scanned for viruses and if required, cleaned.

Don’ts

- Give your Company provided email ID as a contact detail in any free accessible sites unless it is related to your job function.
- Carryout any misuse of the Internet facility in activities such as breach of security or hacking. Download .EXE, .JPG, .AVI, .BMP, .TIF, .VBS, .ZIP, .MPEG, .MP3, .RAR, .ADV, .PPS and .PIF files. This is essential to keep the networks and servers virus-free.

- Download any screen savers, wallpapers, games and/or any entertainment software.
- Access vulgar, pornographic, racist, threatening, and/or violent, or defamatory language/contents under corporate environment.
- Participate in 'Chat rooms' except for any business discussion.
- Download illegitimate and/or license issue software without obtaining clearance from the IT Department. IT system administrator can use the downloading facility only for security patches, evaluation software and updates.
- Use software files, images, or other information downloaded from the Internet that has not been released for free public use
- Transfer or access Spam or chain mails to an 4D E-mail account through the Internet channel.
- Enter into contractual agreements via the Internet; e.g. enter into binding contracts on behalf of the company over the Internet
- Use the company logos or the company materials in any web page or Internet posting unless it has been approved, in advance, by the company management
- Introduce material considered indecent, offensive, or is related to the production, use, storage, or transmission of sexually explicit or offensive items on the company network or systems
- Attempt to gain illegal access to remote systems on the Internet
- Attempt to inappropriately telnet to or port scan remote systems on the Internet
- Use or possess Internet scanning or security vulnerability assessment tools without the permission of the CISO.
- Post material in violation of copyright law
- Establish Internet or other external network connections that could allow other company users to gain access into 4D systems and information assets

7.0 Usage of Email and Communication Activities

Business Use Only

Electronic Mail systems should be used for business purposes only, unless management has specifically approved the non-business use. The language used should be in consistent with other forms of business communication.

The size of file which can be attached to the email is restricted to 35 MB.

Treatment of E-mail as Confidential Information

4D employees should treat electronic-mail messages and files as confidential information. Electronic mail should be handled as a confidential and direct communication between a sender and a recipient.

Management Rights to Review E-mail Content

At any time and without prior notice, 4D management, Information Security officer or Audit team reserve the right to examine e-mail, personal file directories, and other information stored on 4D computers. This examination assures compliance with 4D Security Policy, supports the performance of internal investigations, and assists in the management of 4D information systems.

Restrictions on Transmission of Sensitive Information via E-mail

Users should not send confidential or sensitive information via E-mail unless the material is encrypted using a company approved encryption technique. In case an encrypted channel is not possible for communicating sensitive information, prior management approval on the transmission of the same shall be taken.

Examples include:

- 4D Confidential Information Passwords
- Other confidential or sensitive information

Restrictions on Use of E-mail by the Employees Other than Assigned Individual

Employees of 4D accessing company electronic-mail services should not use or access an electronic-mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on vacation for instance), message forwarding and other facilities should be used instead.

Prohibitions on Automatic Forwarding of E-mail

Unless the information owner / originator agrees in advance, or unless the information is clearly public in nature, employees should not automatically forward electronic mail to any address outside company networks.

Prohibitions on Blanket Forwarding of E-mail

Blanket forwarding of electronic-mail messages to any outside address should be prohibited.

Protection of E-mail due for Legal Purposes

Tape rotation or log destruction of both logs and the referenced electronic-mail messages should be postponed whenever a summons, discovery motion, or other legal notice is received. Such destruction should also be postponed if the material might be needed for an imminent legal action.

Disposal of unneeded Internal Correspondence

While management encourages periodic back-ups of computer-resident information, internal correspondence should be disposed of when no longer needed. Electronic-Mail messages relevant to current activities or that would be expected to become relevant to current activities, should be saved as separate files and retained in accordance with company information retention policies.

4D users must not use email services for any of the following purposes:

- Initiating or propagating 'chain' email or 'pyramid' emails.
- Sending bulk or unsolicited emails, especially of a commercial nature.
- Using their account as a mail-drop for responses for any of the above actions

The following disclaimer shall be displayed on all e-mails send outside 4D domain:

> This e-mail, together with any attachments, is confidential. It may be read, copied and used only by the intended recipient. Access to this e-mail or any of its attachments by anyone else and disclosure or copying of its contents is unauthorized. If you have received this email by mistake, please notify the sender immediately by e-mail or telephone. Please then delete it from your computer without making any copies or disclosing it to any other person. Emails are not secure and may suffer errors, viruses, delay, interception and amendment. Fourth Dimension Technologies Pvt Ltd does not accept liability for any damage caused by the transmission of this email.

8.0 Password Security Policy

Password Management

Confidentiality of Passwords

User passwords should remain confidential and not shared, posted or otherwise divulged in any manner. Passwords shall not be displayed in any environment (including on office walls, desks and workstations) at any time, including during sign-on procedures

Password Composition

Passwords used by 4D employees shall have the following characteristics

1. A minimum of 8 characters.
2. Password should be a combination of Alpha, numeric and one special character. (* ,@ %,$, 1,2,A,B etc..)
3. No portion of the username as part of the password

Password Expiration

Passwords should expire after a maximum period of 90 calendar days. Additionally, the same password should not be repeated within a cycle of 10 password changes.

One Time Use of Initial Passwords

If the administrator provides a user with an initial password, the user should change it immediately after the first-time log – in to the system. (One-time password).

User Capability to Select Passwords

Users should be provided with the capability to change their password on the login interface (after authentication).

Password Reset

User password resets will be performed when requested by the user, after verification of identity.

The ‘Password reset request’ via email should be raised by the user’s Team lead or Team Manager respectively. The new password should be a one-time password. Only the individual to whom the user-ID is assigned should request for user password reset. Security Administrator/ISSO systems should be informed whenever a password is reset for a particular user. In case of request for change of password sent through another user’s login ID, a cc of the mail needs to be sent to the person whose password is being reset.

Screen Saver Password

All users should use the screen saver with password, which should be activated within 5 minutes of inactivity.

Responsibility

It is the responsibility of all users to rigorously follow the password security policy. The users should formally inform the Network Administrator and Security Administrator about any lapse on the password security either orally or by e-mail.

Password Selection Rules

Prohibition of Easy Guess Passwords

Users should be encouraged to create passwords that will prohibit easy guessing (i.e., passwords such as spouse's first name, Children name, etc.).

Examples of good passwords

- Lap$top3
- you@Us1

Passwords should not be based on any of the following: (Best practices)

Bad Examples of password as mentioned below to be avoided as these are easily guessable by any person with malicious intent.

- Months of the year, days of the week or any other aspect of the date (like date of birth, date of joining etc.)
- Name of your spouse, parent, colleague, friend, pet, towns, months, days. Birthdays – of the user or near and dear ones. Number of car/motorbike registration, telephone.

- Employee No. / Employee Id or designations
- Project or department name or references
- Company names, identifiers or references
- Telephone numbers or similar all-numeric groups
- User ID, user name, group ID or other system identifier
- More than two consecutive identical characters
- All-number or all-alphabetic groups
- Common dictionary words
- A series of identical numbers/letters like abcd1234
- Obvious keyboard sequences like asdfgh, qwerty
- Any of the above in inverse or with a number before or after. Password rule

  enforcement procedure

- Passwords of less than 8 characters (10 characters for privileged users) and not containing special characters, Alpha, numerals shall not be allowed. Password minimum duration shall be 24 hours. Passwords shall be valid for 90 days.
- The previous 10 passwords shall not be allowed to be reused.
- Automatic account lockout occurs after 3 consecutive unsuccessful logon attempts by any user.

9.0 Physical Security Policy

Inspection of incoming and outgoing packages

Inspection of incoming and outgoing packages (e.g. bags, briefcases, boxes, laptop computers, etc.) must be conducted to ensure the unauthorized materials are not brought in or taken out of 4D premises. All incoming material should be declared at the security office and a gate-pass document given for clearance of the same. A gate pass duly approved by the respective authority should support any material/ article belonging to 4D, taken out of 4D.

Users physical activity can be monitored through CCTV in work area for emergency and forensic purpose.

Disposal of Media

Equipment which contains sensitive material should be properly discarded or destroyed at the end of its functional life. The equipment used in storing 4D's data, when disposed of, should be done with due consideration and care. Sensitive data, licensed software, and other material should be properly erased or overwritten when destroying or refurbishing and protected when under repair.

It is the responsibility of users to dispose Media containing sensitive information securely.

Following is the list of items that require secure disposal and mode of secure disposal:

- Paper documents: paper shredders should be used
- Carbon paper: paper shredders should be used
- Hard Disk Drives: the HDD should be degaussed/ erased using tools like Zero filling
- Will use Intune for remote wiping
- Compact Disks & DVDs: these should be physically broken or destroyed by means like shredding or incineration.

Server room access

Access to server room is restricted, monitored and on permission by ISSO. All visitors are required to fill and sign in the Server Room Entry Register.

Banned Activities

- Smoking,
- Drinking
- Eating and Chewing.
- Photography

Banned Items

- Bags of any type.
- Cameras
- Removable Memory Devices (Pen Drives, External HDD etc.)
- Laptops
- Electronic Messaging Devices

10.0 Information Security Incidents and Weakness

Security Incident

‘Incident’ is a term related to exceptional situations or a situation that warrants intervention of senior management. An incident is detected in day-to-day operations and management of the IT function. This may be result of unusual circumstances as well as the violations of existing policies and procedures of 4D.

Some examples of Information security incidents

- Suspected hacking attempts
- Successful hacking attempts
- DoS attacks, Ping of Death attacks,
- Port scanning
- Loss of information due to unknown reasons
- Hardware resources and components lost / stolen.

- Virus incidents regarding e-mail, Internet, CD, diskette and others
- Failure / crash of IT equipment
- Power problems and loss of data
- Natural calamity or disaster
- Hardware, Software, and Operational errors that results in erroneous data

Security Weakness

An information security weakness is a condition or circumstance that poses a risk of unauthorized access to confidential information, unauthorized access to 4D computers or networks, damage to or interference with 4D computers or networks, or loss of information.

Some examples of Information security weaknesses

- Known uses of insecure (weak) passwords or sharing of passwords
- Suspicious data flows in or out of a system
- Key logger(s) installed on a desktop or laptop computer
- Systems that are known to be configured in an insecure manner

Users are not supposed to test/exploit security weakness without authorization.

Reporting

Any security incidents noticed by users shall be reported through the following means:

- ➢ Over phone to CISO (8754485958)
- ➢ Over E-mail to incident@fourdtech.co.in

Note: The users should provide the following basic details while reporting:

- Incident Reporter’s name
- Department/Unit
- Actual Incident Date and Time
- Location of incident
- Severity
- Incident Brief Description

The person receiving the information shall fill the incident report form and forward to ISSM/ISSO for necessary action. The ISSM/ISSO must notify the same to the CISO and corrective action must be initiated with the help of Security Team/ Administration team / Security Incident Response Team.

Information Security events shall be reported to outside authorities whenever this is required to comply with legal requirements or regulations. This shall only be done by the persons authorized by CISO in consultation with the legal department.

General

Illegal Usage

Transmission, storage, or distribution of any information, data or material in violation of any applicable law or regulation is prohibited. This includes, but is not limited to: copyrighted material, trademark, trade secret or other intellectual property used without proper authorization, and material that is obscene, defamatory, constitutes an illegal threat.

Security

Violations of system or network security are prohibited, and may result in criminal and civil liability until unless they are authorized to do so. Examples include, but are not limited to the following: Unauthorized access, use, probe, or scan of a systems security or authentication measures, data or traffic; Interference with service to any user, host or network including, without limitation, mail bombing, flooding, deliberate attempts to overload a system and broadcast attacks; Forging of any TCP-IP packet header or any part of the header information in an email or a newsgroup posting.

Usage of Storage Media

Any storage media, not limited to CD-Rom, Pen drive, should be used only after the prior approval of Information Security Steering Committee.

For details refer Media Handling Policy

Further Guidelines

Detailed advice on how to determine and implement an appropriate level of security is available from the Chief Information Security Officer (CISO) or Information System Security Manager (ISSM)

Breach of policy and Enforcement

A breach of this policy could have severe consequences to 4D, its ability to provide services, or maintain the integrity, confidentiality, or availability of services. Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action at the discretion of 4D senior management. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of vendors, termination of their contracted services. All employees and vendors are bound by these policies and are responsible for their strict enforcement.

Acceptable Use of Assets

- Employees, contractors and third party users using or having access to the organization’s assets should be aware of the limits existing for their use of information and assets associated with information processing facilities, and resources. They shall be responsible for their use of any information processing resources, and of any such use carried out under their responsibility.

- The data created on the corporate systems remains the property of the organization.
- Reasonable personal use consistent with conventional ethical standards, of the desktop / intranet and Internet systems by the employees are permitted provided.

The use should not affect 4D business:

- The use should not interfere with employee productivity
- The use should not pre-empt any business activity of 4D.
- The resources should not be used for the personal commercial activities.
- The e-mail facility to be used as per the email security guidelines.
- The mobile devices like Laptop etc. to be used as per the respective security guidelines.

- All critical and vital information must be protected and encrypted, wherever system permits.
- Users should abide the laws on Intellectual property rights such as copy rights, patents, trademarks and source code licenses.

Use of Laptop

Employees are responsible for the security and integrity of information stored on laptop. Users should be aware that the data they create on the corporate systems remains the property of 4D. User responsibility includes regularly saving work onto the shared network drive/OneDrive.

Logging off or locking the Workstation

4D users shall either log off or lock the workstation if they will be away from their desk any length of time. The workstation shall be configured to lock automatically using a secure screen saver if it is not used for a period of 5 minutes.

Personal Work

Computing facilities, services, and networks may not be used for work other than that of 4D.

Clear Screen and Clear desk Policy

- Lock away all confidential and valuable documents (paper and magnetic) in cabinets or desk drawers (as appropriate) when the desk is unattended for an extended period- for example when away for meetings, at lunch times, or overnight
- Log off computers and laptops (unless a password protected screen saver is in operation on the workstation) when unattended. When you have finished a session on the

workstation invoke the password-protected screensaver and at cease of work close down all the applications and log off/shutdown the workstation/laptop and lock the laptop away or secure it through the use of a cable lock

- If, in an emergency, you need to leave the office quickly, e.g. a fire alarm, invoke the password-protected screensaver, so that unauthorized personnel cannot use it .(ONLY IF IT IS SAFE TO DO SO – Remember that Personal safety is more important)
- Keep offices as uncluttered as possible. Unwanted paperwork must not be retained, but disposed of securely (e.g. shredded).

Resources Sharing

There should not be any shared folder created on the local laptop provided to individual users. Users shall be advised not to create any shared folder in their respective laptops. Data on the network or OneDrive shares are secured using Windows permissions and access level controls. All directories and sub-directories, which are shared, shall be protected by proper user authentication and permissions to access with relevant access rights.

Avoid storing passwords or other information that can be used to gain access to other network resources. Computer accounts, passwords, and other types of authorization are assigned to individual Employees who are responsible for its security. Revealing user account password to others or allowing use of user account by others is strictly prohibited. This includes family and other household members when work is being done at home.

Use of privileged access

Special access to information or other special computing privileges is to be used during official duty only. Information that is available through special privileges is to be treated as private & confidential. A deliberate attempt to degrade the performance of a computer system or network or access to any restricted IT Infrastructure is prohibited.

Software Copyright and Licenses

4D shall procure Software licenses to be used in 4D for facilitating its operations. The same needs to be evaluated and approved by ISSO.

Unacceptable Usage activities

- The harmful activities such as creating or propagating viruses; disrupting services; damaging files; intentional destruction or damage to equipment, software, applications, data belonging to 4D or clients; and the like are strictly prohibited.
- Port scanning or security scanning is expressly prohibited unless prior notification to Security Forum.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty, is prohibited.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack) and providing information about, or lists of, 4D employees to parties outside 4D, are prohibited.

- Security breaches or disruptions of network communication, include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties, is prohibited. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Using 4D computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction is strictly prohibited.
- Leaving confidential or sensitive information on printing facilities, photocopiers, and facsimile machines.

Unauthorized access

4D employees shall not:

- Damage computer systems
- Obtain extra resources which are not authorized to an individual
- Deprive another user of authorized resources
- Gain unauthorized access to systems.

By using knowledge of:

- A special password
- Vulnerabilities in computer systems
- Another 4D user’s password
- Accessibility of a 4D user during a previous position or role

User accountability

- Information systems resources are to be used as expressly authorized by administration and management as per the Information Security Policy
- The information systems user is responsible for the general protection of 4D resources.
- Users must be aware that information stored or transmitted through e-mail or via computer, including e-mail, may be subject to disclosure under IT Policy rules.
- Users should have no expectation of privacy for information stored or transmitted using 4D corporate information resources except for records or other information that is confidential.

User role

- Portable computer equipment belonging to the organization should only be used for the organization’s business processing.
- Treat information and associated resources as valuable assets.
- Recognize accountability for improper use of information systems resources.
- Appropriate use of the Internet, Intranet and Extranet apply.

- Report security violations
- Back up personal files and individual software per the Backup and Recovery Policy.
- All files downloaded from the organization (includes internet, and e-mail) must be virus checked before saving to disk. If a virus is detected the files should be immediately deleted, and NOT saved to disk.
- Ensure that if physical locking capabilities are available, these should be applied after office hours.
- Ensure that the theft/loss of a PC is immediately reported to Corporate IT and security department.
- Keep food and drink away from PCs.
- User will be responsible for any accidental damage due to tea, water, or other factors.
- Users must keep the equipment properly cleaned and maintained to the extent that they are able.
- User will be responsible for any accidental damage due to tea, water, or other factors.
- If a theft/loss/damage of IT equipment occurs, the employee will be responsible for reimbursing the loss to 4D, as per the schedule below. The HR Department will be responsible for recovering the cost from the user, based on the report from the ISSC.

A user accepts full responsibility for all violations defined in this document including but not limited to the following situations:

- Users accept full responsibility for all violations that occur on a computer system that has been assigned to that specific user.
- Individual Users are solely responsible for IT Assets allotted to them including but not limited to theft / damage.
- Users are responsible for installing proactive methods to protect their accesses and resources. The Electronic Communications Guidelines provide suggested methods of protection.
- If a user knowingly provides access to others through their 4D corporate network connection, the user is responsible for all violations committed by these persons, and the user will be subject to corrective measures as deemed fit by the HR department.
- Users are responsible for reporting observations of attempted security violations.

Antivirus:

Do’s

- Users should ensure the latest Anti-virus software should be installed on his/her desktop or laptop.
- Users must periodically check the latest definition pattern file version with the help of IT. Users must ‘mark as SPAM’ the junk and/or spam emails that may enter the user’s mailbox. If a user is uncertain as to how to do this, he/she should contact the IT Help Desk.

- If User receive phishing email or impersonation mail should sent mail to Helpdesk, Incident@fourdtech.co.in
- User should scan his/her system regularly and notify to System Administrator if any virus suspected.

Don’ts

- Ignore System Administrator’s Virus warning message at any cost.   Uninstall Anti-virus software.
- Disable the routine scan
- Allow everyone access to any folder. Avoid sharing of local hard drive folders without any proper security and permission.
- Send attachments such as .JPG, .AVI, .VBS, .JPG, .ZIP, .MPEG, .BMP, .RAR, .PPS, .MP3 files to any users within the corporate network or outside.
- Entertain or open any spam or junk mails.
- Download any software or application without scanning.

--End of Document---

Read and Understood