

IT POLICY

Prepared by: <i>TL Bhatnagar</i>	Reviewed by: <i>S. D. Bhatnagar</i>	Approved by: <i>AL</i>
Date: 11/06/2021	Date: 16/06/2024	Date: 17/06/2021

Contents

1. SCOPE.....	3
2. SECURITY POLICIES	3
3. ACCESS CONTROL	4
4. PASSWORD POLICY	4
5. PHYSICAL SECURITY	5
6. SERVER SPECIFIC SECURITY	5
7. WIDE AREA NETWORK SECURITY	6
8. TCP/IP & INTERNET SECURITY	6
9. DATA STORAGE, BACKUP AND RETENTION.....	6
10. DATA TRANSFER.....	6
11. COMPUTER SOFTWARE SYSTEM VALIDATION AND MAINTENANCE.....	6
12. VIRUS PROTECTION.....	6
13. AUDIT TRAIL.....	7
14. INVENTORY MANAGEMENT	7
15. TRAINING	8
16. ABBEVIATIONS.....	8
17. DISTRIBUTION LIST	8
18. VERSION HISTORY	8

Prepared by: <u>RTB</u>	Reviewed by: <u>SDH</u>	Approved by: <u>SDH</u>
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021

1. SCOPE

Interactive Research School for Health Affairs (IRSHA) commits to establish the appropriate use of information technology (IT) system to protect the data integrity, data security, confidentiality and availability of information generated, managed and controlled by the Institute. Use of IT related resources would facilitate management, faculty, students, staffs and visiting guests to protect the information from unauthorized access, disclosure, corruption and loss for the advancement in research, service, and business objectives.

The IT Policy defines regulations and guidelines for proper usage and maintenance of data, proprietary software systems, computer network devices and other related information to ensure their ethical and acceptable use by authorised users and customers.




IRSHA is obligated to

- 1.1 Maintain confidentiality and integrity of data by accessing the IT system as per the password and access control policies.
- 1.2 Provide physical and virus protection to all computer systems, networks and servers.
- 1.3 Provide data storage, backup, and retention as per respective policies at specified interval of time.
- 1.4 Maintain audit trail of work being done with the IT system.
- 1.5 Provide appropriate training to authorized users for handling of IT system.
- 1.6 Ensure the continued availability of data and programs to authorised staff and customers.

IT Resources include computing, networking, communications, application, infrastructure, hardware, software, data, databases, procedures, and any related materials and services.

2. SECURITY POLICIES

- 2.1 Internet and other external service access are restricted to authorized personnel only.
- 2.2 Access to data on all laptop, computers is to be secured by authorization, to provide confidentiality of data in the event of loss. Confidentiality of all data is maintained through access controls
- 2.3 Only authorized and licensed software may be installed, and installation may only be performed by IT Officer or approved vendor.
- 2.4 The use of unauthorized software is prohibited. In the event of unauthorized software being discovered, it will be removed from the workstation immediately.
- 2.5 Computer system configuration settings are handled only by IT Officer.
- 2.6 The physical security of computer system will confirm to recognized loss prevention.
- 2.7 A business continuity plan will be developed and tested on a regular basis.

Prepared by: 	Reviewed by: 	Approved by: 
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021




3. ACCESS CONTROL

- 3.1 All computer system has access control protection. Access is provided to authorize personnel only.
- 3.2 Users requiring access to systems must make a written request by filling User maintenance form
- 3.3 All the user management related activities are created and monitored as per the SOP for User Maintenance in Computer Systems. For example: User Creation, User modification, User deletion etc.
- 3.4 Authorized users are granted required rights to use the system as per defined roles.
- 3.5 The IT Department will control network/server passwords and system passwords is assigned by the IT officer to the end-user. The IT officer is responsible for the maintaining the data integrity of the end-user data and for determining end-user access rights.
- 3.6 IT Team shall oversee and keep all the records regarding the user management activities performed on various systems installed in the organization.
- 3.7 The network/servers and systems is accessed by valid individual username and password.
- 3.8 Usernames and passwords must not be shared by any individual.
- 3.9 User session will be logged off after 10 minutes, if the session is idle for 10 minutes.
- 3.10 The IT department will be notified of any employees leaving the Organization's employment. The IT department will then remove the employee's rights to all systems.
- 3.11 User will not be given access to critical data folder or database and access is provided to IT officer.
- 3.12 Network/server supervisor passwords and IT administrator passwords will be stored in a secure location in case of an emergency or disaster.

4. PASSWORD POLICY

- 4.1 Password policy should be followed by all the employees.
 - Password should be masked
 - Minimum length of 6 characters
 - Maximum age of 180 days, Users shall change their password before expiration period.
 - System shall prompt the users to change their password at the first login after User ID creation.
 - Password should meet password complexity and contain any three combinations from the following four.

English Letters (Upper- or Lower-Case Letters)	A B C ... Z a b c ... z
Numerical	0 1 2 ... 9

Prepared by: 	Reviewed by: 	Approved by: 
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021

Non-alphanumeric ("special characters," symbols)

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

5. PHYSICAL SECURITY

5.1 SERVER ROOM

- 5.1.1 The Server Room has been housed in a specified room with access control and the locking with registered keys is securely kept under supervision.
- 5.1.2 The Server Room contains an adequate air conditioning system to provide a stable operating environment to reduce the risk of system overheating. The temperature in the server room is kept under Manufactures recommended conditions.
- 5.1.3 Redundant power supply with UPS power backup is provided to the computer suite to protect the computer systems in the case of a mains power failure.
- 5.1.4 The server room equipped with ABC fire protection system which will safeguard the servers against fire.
- 5.1.5 All backups and tapes are stored in a secured location with access to authorized personnel only.
- 5.1.6 Access to the server room is restricted to IT department staff and authorized persons from external agency or service providers.
- 5.1.7 All contractors working within the server room are to be supervised at all times and the IT department is to be notified of their presence and provided with details of all work to be carried out.

5.2 HUBS & SWITCHES




LAN equipment, routers, switches will be kept in secure network rack. Access to Network rack will be restricted to IT Department staff only. Other staff and contractors requiring access to hub rooms will be notified to the IT Department in advance to arrange necessary supervision.

5.3 ELECTRICAL SECURITY

Power supply must be provided as per manufacturer's recommendations All servers, workstations, routers, switches and other critical network equipment will be provided with UPS. All UPS will be tested annually.

6. SERVER SPECIFIC SECURITY

- 6.1 The operating system patch update shall be done with recommendation of vendor.
- 6.2 Servers will be checked daily for viruses.
- 6.3 Servers will be locked in a secure room
- 6.4 Users possessing Admin/Administrator/root rights will be limited to trained members of the IT department staff only.
- 6.5 Use of the Admin/Administrator accounts will be kept to a minimum.
- 6.6 User's access to data and applications will be limited by the access control features.

Prepared by: 	Reviewed by: 	Approved by: 
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021

7. WIDE AREA NETWORK SECURITY

- 7.1 Wireless LAN's will make use of the most secure encryption and authentication facilities available.
- 7.2 Unauthorized wireless devices are prohibited.
- 7.3 Where Wireless devices are used, the devices will be unplugged from the network or power off when not in use.
- 7.4 All communication should pass through the Organization's firewall.
- 7.5 All routers and firewalls will be kept locked up in secure areas.
- 7.6 Unnecessary protocols and port will be removed from routers/firewall.
- 7.7 All connections made to the organization's network by outside organizations will be logged Log of VPN login credentials is set for 6 days.

8. TCP/IP & INTERNET SECURITY

- 8.1 Workstation access to the Internet will be via the Organization's firewall and website content scanner.
- 8.2 All the workstations will be linked through intranet for secure data communication/transfer.

9. DATA STORAGE, BACKUP AND RETENTION

- 9.1 Data backup procedures shall be available for Backup, Archival & Restoration of data.
- 9.2 System shall support well defined Backup and Recovery procedure that enables recovery of all complete transaction data in case of system failure.
- 9.3 Backup shall be performed at specified interval of time and all backup copy shall be stored securely.

10. DATA TRANSFER

- 10.1 Inappropriate materials are not allowed to be transmitted by e-mail. As a guide, inappropriate material means anything the organization would not allow printed on Company letterhead paper and sent to a person outside the organization.
- 10.2 Institutional email ID should be used for official communications.
- 10.3 If the message is not from a trusted source, it will be recorded as spam.
- 10.4 Antivirus will be used to scan the mails from viruses.

11. COMPUTER SOFTWARE SYSTEM VALIDATION AND MAINTENANCE

Separate procedure for validation protocol and validation of computer system is prepared as per the regulatory requirements. Provision for annual maintenance contract is facilitated with authorized firm for system maintenance

12. VIRUS PROTECTION

- 12.1 The IT department will possess available up to date virus scanning software for the scanning and removal of suspected viruses.

Prepared by: <i>[Signature]</i>	Reviewed by: <i>[Signature]</i>	Approved by: <i>[Signature]</i>
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021




- 12.2 Site file servers and workstations will be protected with virus scanning software.
- 12.3 Access to external storage device that is from outside the organization shall be restricted.
- 12.4 Original master copies of operating system and software will be used.
- 12.5 All removable media containing executable software (software with .EXE and .COM extensions) will be write protected wherever possible.
- 12.6 New commercial software will be scanned before it is installed as it occasionally contains viruses.
- 12.7 To enable data to be recovered in the event of a virus outbreak, data backup procedure is in place and will be done by IT department.
- 12.8 Management strongly endorses the organization's anti-virus policies and will make the necessary resources available to implement them.
- 12.9 Users will be kept informed of current procedures and policies and training will be provided for the required personnel.
- 12.10 Users will be notified of virus incidents.
- 12.11 All concerned personnel will be accountable for any breaches of the organization's anti-virus policies.
- 12.12 In the event of a possible virus infection, the user must inform to IT Officer immediately on E-mail tushar.bhosale@bharativedyapeeth.edu. IT Department will take necessary and appropriate action to stop the virus spread and eradicate it.

13. AUDIT TRAIL

- 13.1 Audit Trail of computer applications installed in the laboratory should be in a human readable format.
- 13.2 Periodic review of audit trail shall be done by Quality Assurance Team.
- 13.3 The audit trail report shall be secured and non-editable to all including the IT administrator.
- 13.4 The system users including administrator must not be capable of disabling the audit trail functionality.

14. INVENTORY MANAGEMENT

- 14.1 The IT Department will keep a full inventory of all computer equipment and software in use throughout the organization.
- 14.2 Computer hardware and software audits will be carried out periodically via the use of a desktop inventory package.
- 14.3 These audits will be used to track unauthorized copies of software and unauthorized changes to hardware and software configurations.

Prepared by: 	Reviewed by: 	Approved by: 
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021

15. TRAINING

All staff authorized to use the Organizations computer system will receive appropriate training before using the system and training will be updated as required.

16. ABBEVIATIONS

HOD	Head of Department
ID	Identification
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MAC	Media Access control
SOP	Statement of Purpose
TCP	Transmission Control Protocol
UPS	Uninterrupted Power Supply


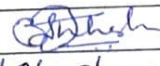

17. DISTRIBUTION LIST

Name/Location	Copy No.	Distribution
Master Copy	01	Quality Manager
Controlled Copy	02	Laboratory Manager
Controlled Copy	03	IT Officer

18. VERSION HISTORY

Version No	Version date	Reason for amendment
01		Initial Release

*****End of Section *****

Prepared by: 	Reviewed by: 	Approved by: 
Date: 11/06/2021	Date: 16/06/2021	Date: 17/06/2021