



DR. BABASAHEB AMBEDKAR
OPEN UNIVERSITY

INFORMATION TECHNOLOGY POLICY
(IT POLICY)

1 Table of Contents

1	Domain Account Management Policy	5
1.1	Purpose:	5
1.2	Scope of Domain Account Management Policy	5
2	Antivirus Policy.....	6
2.1	Purpose	6
2.2	Scope.....	6
2.3	General Policy	6
2.4	Rules for Virus Prevention.....	7
2.5	Computer Department Responsibilities	8
2.6	Department and Individual Responsibilities	9
2.7	Enforcement.....	9
3	Audit Policy (Internal).....	10
3.1	Purpose:	10
3.2	Audits can be conducted to:	10
3.3	Scope of Audit Policy:	10
4	Change Management Policy.....	11
4.1	Purpose:	11
4.2	Scope of Change Management Policy:.....	11
5	End-User Backup Policy	12
5.1	Introduction	12
5.2	Scope.....	12
5.3	Backup Schedule.....	12
5.4	Data Storage.....	12
5.5	Managing Restores	13
6	Computer Network and Internet Use Policy	15
6.1	Personal Responsibility	15
6.2	Term of Permitted Use	15
6.3	Purpose and Use.....	15
6.4	Netiquette Rules	15
6.5	Banned Activity	15
6.6	Summary internet usage policy provisions	16
7	Copyright on Digital Information Systems	18
7.1	Introduction	18
7.2	Notification of Infringement	18
7.3	Removal of Infringing Material	19
7.4	Designation of Agent to Receive Notification of Claimed Infringement.....	21

7.5	Indemnification of Dr. Babasaheb Ambedkar Open University	21
7.6	Noncompliance and Sanctions.....	22
7.7	Malicious misuse. Examples	22
7.8	Unacceptable use of software and hardware	22
7.9	Inappropriate access	22
7.10	Inappropriate use of electronic mail and Internet access.....	23
7.11	Submission of Copyrighted Work.....	23
7.12	Enforcement.....	24
8	Desktop Remote Access Policy.....	25
8.1	Purpose	25
8.2	Scope.....	25
9	Email Policy.....	27
9.1	Introduction	27
9.2	Bulk Mail	27
9.3	Email Monitoring	27
9.4	Email Privacy.....	28
9.5	Personal E-mail	28
9.6	Authorized Personal E-mail Use	28
9.7	Employees Have No Reasonable Expectation of Privacy.....	28
9.8	E-mail Monitoring Activities	29
9.9	Offensive Content and Harassing or Discriminatory Activities Are Banned.....	29
9.10	Prohibition.....	29
	Employees Are Prohibited from Using E-mail to:	29
9.11	Confidential, Proprietary, and Personal Information Must Be Protected.....	30
9.12	Violations	30
10	Equipment Borrowing Policy	31
10.1	IT Equipment may be borrowed:	31
10.2	To borrow IT equipment, proper procedures must be done:.....	31
10.3	Privileges to borrow IT equipment may be revoked or suspended due to the following:	31
10.4	To book required IT equipment, visit the Computer Department.	31
11	ERP Data Protection Policy	32
11.1	PURPOSE	32
11.2	POLICY.....	32
11.3	APPLICABILITY	33
11.4	SANCTIONS.....	33
12	Information Disclosure Policy.....	34
12.1	Purpose:	34

12.2	Scope of Information Disclosure Policy:	34
12.3	Scope of Information Disclosure Policy:	34
12.4	Email Disclaimer Message.....	35
13	Intranet Policy.....	36
13.1	Purpose:	36
13.2	Scope of Intranet Policy	36
14	Intrusion Detection Policy	37
14.1	Purpose:	37
14.2	Scope of Intrusion Detection Policy:	37
15	IT Asset Policy.....	38
15.1	Purpose:	38
15.2	Scope of IT Asset Policy:	38
16	IT Asset Disposal Policy.....	39
16.1	Purpose	39
16.2	Scope.....	39
16.3	Definitions	39
16.4	Guidelines.....	40
16.5	Practices.....	40
16.6	Policy	40
16.7	Income Derived from Disposal:.....	41
16.8	Assets beyond reasonable repair:	41
16.9	Decommissioning of Assets:.....	42
16.10	Donations:	42
17	Network Security Policy for Portable Computers	43
17.1	Introduction	43
17.2	Protecting the Laptop	43
17.3	Laptop User's Responsibilities	43
17.4	Security Audits.....	44
18	Password Security Policy.....	45
18.1	Purpose	45
18.2	Scope of Password Security Policy	45
19	Printer Policy	46
19.1	Purpose	46
19.2	Scope.....	46
19.3	Supported Printers.....	46
19.4	General Policy	46
20	Removable Media Acceptable Use Policy.....	49
20.1	Scope.....	49

20.2	Usage.....	49
20.3	Applicability	50
20.4	Affected Technology.....	51
20.5	Policy and Appropriate Use.....	51
20.6	Access Control	51
20.7	Security.....	52
20.8	Help & Support	54
20.9	Organizational Protocol	54
20.10	Policy Non-Compliance	55
21	Reporting Critical Service Outages During Academic Term	56
21.1	56
22	Server Security Policy	58
22.1	Purpose:	58
22.2	Scope of Secure Policy:	58
23	Software Licensing Policy	59
23.1	Purpose:	59
23.2	Scope of Secure Policy:	59
24	Tablets/Smartphone Usage Policy	60
24.1	Purpose	60
24.2	Scope.....	61
24.3	Supported Technology	61
24.4	Eligible Users.....	62
24.5	Policy and Appropriate Use.....	62
24.6	Policy Non-Compliance	66
25	Wireless Security Access Policy.....	67
25.1	Purpose	67
25.2	Scope.....	67
25.3	Supported Technology	68
25.4	Eligible Users.....	69
25.5	Policy and Appropriate Use.....	69

1 Domain Account Management Policy

1.1 Purpose:

The purpose of this policy is to define guidelines for the creation, monitoring, control and removal of domain user accounts.

1.2 Scope of Domain Account Management Policy

1.2.1. All accounts are created when associated request and approval comes from New user duly endorsed by his HOD and HR Department.

1.2.2. All accounts have following policy enabled on domain wide perspective (System Login Account)

1.2.3. Enforce password history : 05

1.2.4. Max. Password Age : 90 Days

1.2.5. Min. password length : 06 Characters

1.2.6. Account lockout duration : 30 minutes

1.2.7. Account lockout threshold : 05 invalid logon attempts

1.2.8. Reset account lockout counter : 30 minutes

2 Antivirus Policy

2.1 Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CDs. Viruses are usually disguised as something else, and so their presence is not always obvious to the computer user. A virus infection can be very costly to Dr.BabasahebAmbedkar Open University in terms of lost data, lost staff productivity, and/or lost reputation.

As a result, one of the goals of Dr.BabasahebAmbedkar Open University is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by Dr.BabasahebAmbedkar Open University employees to help in achieving effective virus detection and prevention.

2.2 Scope

This policy applies to all computers that are connected to the Dr.BabasahebAmbedkar Open University network via a standard network connection, wireless connection, modem connection, or virtual private network connection. This includes both University-owned computers and personally owned computers attached to the Dr.BabasahebAmbedkar Open University network. The definition of computers includes desktop workstations, laptop computers, handheld computing devices (PDAs)/Smartphones, and servers.

2.3 General Policy

2.3.1. Currently, Dr. BabasahebAmbedkar Open University has Seqrite Endpoint Security by Quick Heal Technologies Ltd.As anti-virus software in use. Licensed copies of Seqrite Endpoint Security anti-virus software can be obtained from the Computer Department. The most current available version of the anti-virus software package will be taken as the default standard.

2.3.2. All computers attached to the Dr. BabasahebAmbedkar Open University network must have standard, supported anti-virus software installed. This software must be active and scheduled to

perform virus checks at regular intervals, and have its virus definition files kept up to date.

- 2.3.3. Dr. Babasaheb Ambedkar Open University requires all existing and incoming students to install anti-virus software on their personal computers by the end of the second week of classes each semester. Failure to do so can result in the loss of connectivity to the Dr. BabasahebAmbedkar Open University network until anti- virus software is installed. Microsoft Fore Front anti- virus software is provided free to all students. Other anti-virus products may be substituted as long as they are kept current.
- 2.3.4. Any activities with the intention to create and/or distribute malicious programs onto the Dr. BabasahebAmbedkar Open University network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.
- 2.3.5. If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the Computer Department immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
- 2.3.6. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the Computer Department.
- 2.3.7. Any virus-infected computer will be removed from the network until it is verified as virus-free.

2.4 Rules for Virus Prevention

- 2.4.1. Always run the standard anti-virus software provided by Dr. BabasahebAmbedkar Open University.
- 2.4.2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.
- 2.4.3. Never open any files or macros attached to an e-mail from a known source (even a co-worker) if you were not expecting a specific attachment from that source.

- 2.4.4. Be suspicious of e-mail messages containing links to unknown Websites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.
- 2.4.5. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.
- 2.4.6. Avoid direct disk sharing with read/write access. Always scan a removable device for viruses before using it.
- 2.4.7. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.
- 2.4.8. Back up critical data and systems configurations on a regular basis and store backups in a safe place.
- 2.4.9. Regularly update virus protection on personally owned home computers that are used for business purposes. This includes installing recommended security patches for the operating Systems and other applications that are in use.

2.5 Computer Department Responsibilities

The following activities are the responsibility of the Dr.BabasahebAmbedkar Open UniversityComputer Department:

- 2.5.1. The Computer Department is responsible for maintaining and updating this Anti-Virus Policy.
- 2.5.2. The Computer Department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software version in use.
- 2.5.3. The Computer Department will apply any updates to the services it provides that are required to defend against threats from viruses.
- 2.5.4. The Computer Department will install anti-virus software on all Dr. BabasahebAmbedkar Open University owned and installed desktop workstations, laptops, and servers.
- 2.5.5. The Computer Department will take appropriate action to contain, remove, and assist in recovery from virus infections. In order to do so, the Computer Department may be required to disconnect a

suspect computer from the network or disconnect an entire segment of the network.

2.5.6. The Computer Department will perform regular anti-virus sweeps.

2.5.7. The Computer Department will attempt to notify users of Dr. BabasahebAmbedkar Open University systems of any credible virus threats via e-mail or telephone messages. Virus reports will not be acted upon until validated. Employees should not forward these or any virus warning messages in order to keep network traffic to a minimum.

2.6 Department and Individual Responsibilities

The following activities are the responsibility of Dr.BabasahebAmbedkar Open University departments and employees:

2.6.1. Departments must ensure that all departmentally managed computers have virus protection that is in keeping with the standards set out in this policy.

2.6.2. Departments that allow employees to use personally-owned computers for official purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

2.6.3. All employees are responsible for taking reasonable measures to protect against virus infection.

2.6.4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the Dr.BabasahebAmbedkar Open University network without the express consent of the Computer Department.

2.7 Enforcement

Any employee or student who is found to have violated this policy are subject to the Employee/Student Conduct Code and may be subject to disciplinary action, up to and including termination of employment/school.

3 Audit Policy (Internal)

3.1 Purpose:

To provide the authority for members of IU's security forum to conduct a security audit on any system on IU's IT infrastructure at campus.

3.2 Audits can be conducted to:

- 3.2.1. Ensure integrity, confidentiality and availability of information and resources.
- 3.2.2. Investigate possible security incidents, ensure conformance to IU's security Policies
- 3.2.3. Monitor user or system activity if required.

3.3 Scope of Audit Policy:

- 3.3.1. A periodic audit will be conducted to check all the policies.
- 3.3.2. During audit, system and user level access to any computing or communicating device will be provided to the auditors.
- 3.3.3. At the end of every three-month, security forum will research all of the requirements pertaining to the area to be audited.
- 3.3.4. All audits will be documented in the audit report.
- 3.3.5. A follow up audit will be done after 30 days to determine the effectiveness of corrective actions.

4 Change Management Policy

4.1 Purpose:

The purpose of change management is to maintain and improve system integrity; availability; confidentiality and functionally with the IU's information processing infrastructure

4.2 Scope of Change Management Policy:

- 4.2.1. All changes to application software, system software, hardware, network and data in the system will be authorized in nature.
- 4.2.2. The authorization procedures for changes will be documented.
- 4.2.3. Changes will be itemized in different priorities to conduct them in their respective time period.
- 4.2.4. High priority changes will be attended within 2 days, medium priority changes are attended within 7 days and low priority changes are attended within 15 days.
- 4.2.5. Version changes of application software, system software will be documented.
- 4.2.6. Before making the changes, proper analysis will be done to ascertain the impacts on the operational system and its functionality.

5 End-User Backup Policy

5.1 Introduction

Data is one of Dr.BabasahebAmbedkar Open University's most important assets. In order to protect this asset from loss or destruction, it is imperative that it is safely and securely captured, copied, and stored. The goal of this document is to outline a policy that governs how and when data residing on University desktop computers, PCs, and Laptops - as well as home office/mobile devices and appliances - will be backed up and stored for the purpose of providing restoration capability. In addition, it will address methods for requesting that backed up data are restored to individual systems.

5.2 Scope

This policy refers to the backing up of data that resides on individual PCs, notebooks, laptop computers, and other such devices (to be referred to as "workstations").

Responsibility for backing up data on local desktop systems or laptops rests solely with the individual user. It is imperative that end-users save their data to the appropriate media and/or network space outlined in this policy in order that their data is backed up regularly in accordance with University regulations and business continuity plans.

This policy does not cover end-user information that is saved on a network or shared drive, as these are backed up when the servers are backed up.

5.3 Backup Schedule

Backups are conducted on every Friday.

5.4 Data Storage

It is Dr.BabasahebAmbedkar Open University's policy that ALL data of Dr.BabasahebAmbedkar Open University will be backed up according to schedule. This includes any University, applications/projects under development, Website collateral, graphic designs, and so on, that reside on end-user computers.

- 5.4.1. **Office Users:** Dr. Babasaheb Ambedkar Open University data, especially works-in-progress, should be saved. This ensures that data will be backed up when the servers are backed up. If data is saved on a workstation's local drive, then that must be backed up every week onto their mapped network drive.
- 5.4.2. **Remote/Mobile Users:** Remote and mobile users will also back up data and then follow the same procedure as "Office Users" shown above. If this is not feasible due to distance from their office, then the remote/mobile user will employ CD/DVD Read/Write disks. **Should Read/Write disks not be available, then select files should be copied to some type removable storage device** as per Removable Device Policy, such as a mini hard drive, or solid state memory card.

5.5 Managing Restores

The ultimate goal of any backup process is to ensure that a restorable copy of data exists. If the data cannot be restored, then the process is useless. As a result, it's essential that the IT Department regularly test its ability to restore data from the storage media or network drive. As such, all storage media must be tested time to time (3 to 4 times a year) to ensure that the data they contain can be completely restored to end-user workstations. Data will be restored from a backup if:

- 5.5.1. There is an intrusion or attack.
- 5.5.2. Files have been corrupted, deleted, or modified.
- 5.5.3. Information must be accessed that is located on an archived backup.
- 5.5.4. That workstation belongs to a domain.

In the event that an end-user requires or desires a data restore, the following policy will be adhered to:

- 5.5.5. The individual responsible for overseeing backup and restore procedures is Manager of Computer Department. If a user has a restore request, they can contact Computer Department by sending an e-mail, or filling out and submitting a request form.

5.5.6. In the event of unplanned downtime, attack, or disaster, Dr.BabasahebAmbedkar Open University's full restoration procedures will take place.

5.5.7. In the event of a local data loss due to human error, the end-user affected must contact the Computer Department and request a data restore. The end-user must provide the following information:

- Name.
- Contact information.
- Name of file(s) and/or folder(s) affected.
- Last known location of files(s) and/or folder(s) affected.
- Extent and nature of data loss.
- Events leading to data loss, including last modified date and time (if known).
- Urgency of restore.

5.5.8. If the data loss was due to user error or a lack of adherence to procedure, then the responsible end-user may be required to participate in a tutorial on effective data backup practices and disciplinary action may be taken against those who are found to be repeatedly not adhering to backup procedures.

6 Computer Network and Internet Use Policy

6.1 Personal Responsibility

By accepting your account password and related information and accessing DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's network or Internet Systems, you agree to adhere to this policy. You also agree to report any network or Internet misuse to the Director of Computer Department. Misuse includes policy violations that harm another person or another individual's property.

6.2 Term of Permitted Use

Network and Internet access extends throughout the term of your employment, provided you do not violate the organization's computer network and Internet use policy. Note: DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY may suspend access at any time for technical reasons, policy violations, or other concerns.

6.3 Purpose and Use

The university offers access to its network and Internet Systems for official/academic purposes only. If you are unsure whether an activity constitutes appropriate official/academic use, consult either HOD or Head of Computer Department.

6.4 Netiquette Rules

Employees must adhere to the rules of network etiquette, or netiquette. In other words, they must be polite, adhere to the organization's electronic writing and content guidelines, and use the network and Internet appropriately and legally. DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY will determine what materials, files, information, software, communications, and other content and activity are permitted or prohibited, as outlined below.

6.5 Banned Activity

The following activities violate DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's computer network and Internet use policy:

- 6.5.1. Using, transmitting, receiving, or seeking inappropriate, offensive, vulgar, suggestive, obscene, abusive, harassing, belligerent, threatening, defamatory (harming another person's reputation by lies), or misleading language and materials.

- 6.5.2. Making ethnic, sexual-preference, or gender-related slurs or jokes.
- 6.5.3. Engaging in illegal activities, or encouraging others to do so.

6.6 Summary internet usage policy provisions

- 6.6.1. The University has software (Cyberoam) and systems in place that can monitor and record all Internet usage.
- 6.6.2. We reserve the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
- 6.6.3. No Employee should use the TOR browser or any of its variants to bypass security systems in any form. Employee found using TOR application or similar browser or its variants will be considered as a serious offense and result will in the suspension, disciplinary action, and possibly termination.
- 6.6.4. Sexually explicit material should not be displayed, archived, stored, distributed, edited or recorded using our network or computing resources.
- 6.6.5. Use of any University resources for illegal activity is grounds for immediate dismissal, and we will cooperate with any legitimate law enforcement activity.
- 6.6.6. No employee should use University facilities knowingly to download or distribute pirated software or data.
- 6.6.7. No employee should use the University Internet facilities to deliberately propagate any virus, worm, Trojan horse or trap-door program code etc.
- 6.6.8. In the interest of keeping the University well-informed, use of YouTube Education videos is acceptable, provided they are relevant to the scope of our academic curriculum.

- 6.6.9. Employees with Internet access should not use University Internet facilities to download entertainment software or games, or to play games against opponents over the Internet.
- 6.6.10. No employee is allowed to visit video/music streaming websites for entertainment purpose. Only YouTube streaming is allowed with education filter.
- 6.6.11. Each employee using the Internet facilities of the University will have to identify himself or herself honestly, accurately and completely, when setting up accounts on outside computer systems.
- 6.6.12. Only those employees or officials who are authorized to speak to the media, to analysts or at public gatherings on behalf of the University may speak/write in the name of the University in any electronic communications. Where an individual participant is identified as an employee of the University, the employee must refrain from any political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the University of any commercial product or service not sold or serviced by this University.
- 6.6.13. Employees are reminded that it is inappropriate to reveal confidential information, and any other material covered by existing University secrecy policies and procedures on the Internet. Employees releasing such confidential information—whether or not the release is inadvertent — will be subject to the penalties provided in existing University policies and procedures.
- 6.6.14. User IDs and passwords help maintain individual accountability for Internet resource usage. Any employee who obtains a password or ID for an Internet resource from University must keep that password confidential. University policy prohibits the sharing of user IDs or passwords obtained for access to Internet sites. Employees/Student found repeatedly ignoring this policy will be subjected to disciplinary action.

7 Copyright on Digital Information Systems

7.1 Introduction

Individuals using computers and networks ("Digital Information Systems") at Dr.BabasahebAmbedkar Open University (the "University") are responsible for complying with copyright laws and the University's policies and procedures regarding use of the Digital Information Systems. The University reserves the right to deny, limit, revoke or extend computing privileges and access to the Digital Information Systems at Computer Department discretion. In addition, alleged violations of this procedure, the University's policies regarding use of the Digital Information Systems, or other policies of the University in the course of using the Digital Information Systems may result in an immediate loss of computing privileges and may also result in the referral of the matter to the University's Management.

The procedures outlined below will apply when the University receives notification of an alleged copyright infringement. For purposes of these procedures, an E-mail message shall be considered a written notice or request.

7.2 Notification of Infringement

7.2.1. Copyright holders who believe their copyrighted material has been infringed by an account holder must notify the University's Executive President or the competent authority (Registrar) of the allegedly infringing action or material in writing. The notification must:

7.2.1.1. Identify the copyrighted material being infringed in sufficient detail to permit the University to locate the allegedly infringing material on the University's Digital Information Systems,

7.2.1.2. State the basis for the claim of possible infringement,

7.2.1.3. State the basis for the copyright holder's copyright in the work (e.g., author, owner, and assignee).

- 7.2.2. The Registrar will notify the account holder who appears to have posted the allegedly infringing material, and will investigate the complaint promptly.
- 7.2.3. If, after conducting an investigation, the Computer Department or Registrar determines that the allegedly infringing material appears to infringe the copyright of the copyright holder, the Registrar will follow the procedures for Removal of Infringing Material set forth below.

7.3 Removal of Infringing Material

- 7.3.1. In the event that the allegedly infringing material is being used for an active class at the University, the Registrar will attempt to work out an arrangement with the copyright holder for use of the allegedly infringing material by the account holder until the end of the current semester. Failing a satisfactory arrangement, the Registrar will conduct an investigation of the incident and take action as set forth below regarding any allegedly infringing material.
- 7.3.2. If, after the Registrar's investigation, the Registrar determines that the allegedly infringing material appears not to infringe the copyright of the copyright holder, the Registrar will notify the copyright holder and the account holder of the determination. If the copyright holder disagrees with the determination of the Registrar, the copyright holder may request in writing that the University may appoint a lawyer to render an opinion as to whether the allegedly infringing material constitutes copyright infringement pursuant to paragraph below.
- 7.3.3. If, after the Registrar's investigation, the Registrar determines that the allegedly infringing material appears to infringe the copyright of the copyright holder, the Registrar will notify the Executive President of Dr.BabasahebAmbedkar Open University, the copyright holder and the account holder whose account was used to post the allegedly infringing material.

- 7.3.4. Upon receipt of such notification from the Registrar, the Executive President of Dr.BabasahebAmbedkar Open University, will direct the appropriate Computer Department staff member to remove, or block access to, the allegedly infringing material.
- 7.3.5. Upon receipt of notification from the Registrar that the allegedly infringing material appears to infringe the copyright of the copyright holder and is being blocked or removed from IU Digital Information Systems, the account holder may request that the Designated Representative restore the removed or blocked material based on the account holder belief that the allegedly infringing material is not infringing. Such request must be in writing and include a detailed statement of the basis for the account holder's belief that the allegedly infringing material is not infringing, as well as a request that the removed or blocked material be restored.
- 7.3.6. If the Registrar receives such request from the account holder, the Registrar will provide a copy of the request to the copyright holder.
- 7.3.7. If, within 15 working days after a copy of the account holder's request is sent to the copyright holder by the Registrar, the Registrar has not received a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material, the Registrar will notify the Executive President, Dr.BabasahebAmbedkar Open University to restore the material. The Executive President of Dr.BabasahebAmbedkar Open University, will restore the allegedly infringing material within four working days after receipt of such notification.
- 7.3.8. If the Registrar receives within 15 working days a written request from the copyright holder to continue the blocking or removal of the allegedly infringing material is received from the original

sender, the Registrar will provide copies of all correspondence in the matter to the Executive President of Dr.BabasahebAmbedkar Open University, who will forward copies of such correspondence to the University's lawyer, who will be asked to render an opinion as to whether the allegedly infringing material constitutes copyright infringement. If the allegedly infringing material is determined not to constitute copyright infringement, the material will be restored by the Executive President, within four working days of such determination.

7.4 Designation of Agent to Receive Notification of Claimed Infringement

- 7.4.1. This is to notify copyright holders that Dr.BabasahebAmbedkar Open University's Registrar to receive notices and requests concerning claimed infringement, pursuant to the Indian Copyright Act, 1957 is **Executive President**. Any copyright holder wishing to send a notice to Dr.BabasahebAmbedkar Open University regarding possible copyright infringement should file that notice in writing with Executive President at the following address:

Executive President

Dr.BabasahebAmbedkar Open University,
'Jyotirmay' Parisar,Sarkhej-Gandhinagar Highway,
Chharodi, Ahmedabad - 382 481.

7.5 Indemnification of Dr. BabasahebAmbedkar Open University

Users agree, in consideration of access to the University's computing, networking and media services, to indemnify, defend, and hold harmless the University for any lawsuits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the University's computing, networking, and media services and facilities.

7.6 Noncompliance and Sanctions

Information Technology Services may suspend or terminate all computing privileges of any individuals without notice who engage in improper computing activities. Serious cases, as determined by the President of Dr.BabasahebAmbedkar Open University, will be referred to the Board of Management for disciplinary action. Such disciplinary action may include the suspension, expulsion, or termination of the offending individual, as appropriate and as determined at the sole discretion of Dr.BabasahebAmbedkar Open University. Where violation of law is involved, cases will be referred to the proper legal authorities for action. The following serves to provide examples of violations of computing or computing facility policies at Dr.BabasahebAmbedkar Open University. The list of violations includes, but is not limited to.

7.7 Malicious misuse. Examples

Using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from public computers, spreading viruses, sending email that threatens or harasses other people, invading the privacy of others, and subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their approval.

7.8 Unacceptable use of software and hardware

Examples: knowingly or carelessly running or installing unlicensed software on any computer Systems or network; giving another user a program intended to damage the Systems; running or installing any program that places an excessive load on a computer Systems or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

7.9 Inappropriate access

Examples: unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus

network to gain unauthorized access to any computer Systems; connecting unauthorized equipment to the campus network; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers, terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.


7.10 Inappropriate use of electronic mail and Internet access

Email communications are subject to statements of conduct as published in the Student, Faculty, Administrator, Staff, and Maintenance and Operations Handbooks, as well as all applicable IT Act, 2000 and IT (Amendment) Act, 2008. In addition, other activities that threaten the integrity of the Systems or harm individual users are not allowed. These include, but are not limited to initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to news groups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous email; using another person's email account or identity to send email messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using email or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

7.11 Submission of Copyrighted Work

No employee of Dr.BabasahebAmbedkar Open University may reproduce any copyrighted work in violation of the law. Copyrighted works include, but are not limited to: text (e.g. articles), images (e.g. photographs), graphics (e.g. logos), sound recordings (e.g. MP3s, .wav), video recordings (e.g. movies), or software programs.

If a work is copyrighted, you must seek out and receive express written permission of the copyright holder to reproduce the copyrighted work in order to avoid violation. This also includes all copyrighted works held by



Dr.BabasahebAmbedkar Open University in order to get permission to copy or reproduce Dr.BabasahebAmbedkar Open University's copyrighted materials.

7.12 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination.

8 Desktop Remote Access Policy


8.1 Purpose

To control remote access to a University computer desktop from a remote location.

8.2 Scope

All employees and faculty members with a University owned Systems that resides on a University controlled network.

- 8.2.1. All persons needing remote access to their University desktop (e.g. to work from home, access from a conference, etc.) must use only University approved software that is installed by Computer Department of Dr.BabasahebAmbedkar Open University to remotely gain access to these systems.
- 8.2.2. The current University standard remote desktop access software is through Open VPN.
- 8.2.3. Any employee requesting remote access must have an Executive President, direct report to Vice President, or Dean's approval to obtain and use this software,
- 8.2.4. Requests for the use of this software cannot be self-approved. In the event that you are requesting this software installed on your computer and you are at the level in which you can approve installation of the software, that request will be approved by the IT Security Office.
- 8.2.5. All employees are prohibited from installing remote access software on their desktops, unless specifically directed by Computer Department, Dr.BabasahebAmbedkar Open University. Examples of remote access software include, but are not limited to unauthorized copies of LogMeIn, GoToMyPC, TeamViewer etc.



8.2.6. Computer Department, Dr.BabasahebAmbedkar Open University will remove any unauthorized remote desktop software installed on a University-owned Systems on a University controlled network.

9 Email Policy

9.1 Introduction

Any User's use of the University's e-mail Systems, like all of the IT Resources, is to be used only in support of our educational, research, and administrative mission and must be in conformity with the general IT Policy and compliant with all applicable law. Accordingly, Users must use this resource in an efficient, effective, ethical, and lawful manner. E-mail communications should reflect, rather than undermine, the University's reputation and standard of excellence. Violation of the E-mail Policy may result in disciplinary actions and not limited to termination of employee.

9.2 Bulk Mail

In addition to the User's obligation to adhere to the Anti-Spam Policy, Users are prohibited from sending mass or bulk e-mails or messages to other Users if such e-mails or messages do not further the University's goals, interests, or educational mission. For the purposes of this policy, "mass" or "bulk" e-mails or messages include, but are not limited to, any such e-mail or message that is sent to:

- 9.2.1. More than 10 recipients;
- 9.2.2. Any number of undisclosed recipients;
- 9.2.3. One or more pre-defined group of e-mail addresses or list addresses which distribute(s) the e-mail or message to all Users within the group(s); and
- 9.2.4. Any number of recipients if the identity of the sender is undisclosed or masked.

9.3 Email Monitoring

All network and e-mail accounts maintained on and through the IT Resources are the sole properties of the University. The University has the right, but not the obligation, to monitor any e-mail account for legitimate academic reasons. Reasons for review include, but are not limited to:

- 9.3.1. Reasonable suspicion of a violation of the IT Policy or any other rule, law, or property right of another User or third party;
- 9.3.2. Investigation of Systems problems;

- 9.3.3. Litigation or anticipated litigation; or
- 9.3.4. Any other technical or legal obligation or responsibility.

9.4 Email Privacy

To the greatest extent possible, the University will attempt to preserve the privacy of any User whose e-mail account is accessed or monitored. However, Users of the University's e-mail Systems must understand that all communications created, received, archived, or backed-up through the IT Resources may be subject to requests for public disclosure. Accordingly, Users should have no absolute expectation of privacy or confidentiality for data, documents, messages, and other materials stored or transmitted on or through the IT Resources, including via e-mail accounts.

9.5 Personal E-mail

Employees are prohibited from using personal e-mail software (e.g., Gmail, Yahoo!, Hotmail, or etc.) for academic or personal communications at the office.

9.6 Authorized Personal E-mail Use

Employees may use e-mail to communicate with spouses, children, and other family members. Employees' personal use of e-mail is limited to lunch breaks and work breaks only. Employees may not use e-mail for personal purposes during productive business hours. Employees are prohibited from using e-mail to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

9.7 Employees Have No Reasonable Expectation of Privacy

E-mail messages created and transmitted on Dr.BabasahebAmbedkar Open University's computers are the property of Dr.BabasahebAmbedkar Open University. Dr.BabasahebAmbedkar Open University reserves the right to monitor all e-mail transmitted via the Dr.BabasahebAmbedkar Open University's computer Systems. Employees have no reasonable expectation of privacy when it comes to business and personal use of Dr.BabasahebAmbedkar Open University's e-mail Systems.

9.8 E-mail Monitoring Activities

Dr.BabasahebAmbedkar Open University reserves the right to monitor, inspect, copy, review, and store any and all employee e-mail use at any time and without prior notice. In addition, Dr.BabasahebAmbedkar Open University may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through the Dr.BabasahebAmbedkar Open University's e-mail Systems. Dr.BabasahebAmbedkar Open University reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

9.9 Offensive Content and Harassing or Discriminatory Activities Are Banned

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

9.10 Prohibition

Employees Are Prohibited from Using E-mail to:

- 9.10.1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, colour, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
- 9.10.2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
- 9.10.3. Spread gossip, rumours, or innuendos about employees, clients, suppliers, or other outside parties.
- 9.10.4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
- 9.10.5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.
- 9.10.6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass

Dr.BabasahebAmbedkar Open University, negatively impact employee productivity, or harm employee morale.

9.11 Confidential, Proprietary, and Personal Information Must Be Protected

Unless authorized to do so, employees are prohibited from using e-mail to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about Dr.BabasahebAmbedkar Open University, its employees, students, suppliers, and other business associates. Confidential information includes, but is not limited to, client lists, credit card numbers, PAN Card numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass Dr.BabasahebAmbedkar Open University and its employees if the information were disclosed to the public.

9.12 Violations

These guidelines are intended to provide Dr.BabasahebAmbedkar Open University employees with general examples of acceptable and unacceptable uses of the company's e-mail Systems. A violation of this policy may result in disciplinary action up to and including termination.

10 Equipment Borrowing Policy

Borrowers are responsible for loss or damage to equipment

Equipment that is not picked up within the one hour of the booked time may be loaned to others. A minimum of 1 week's advance notice is requested to ensure equipment availability.

10.1 IT Equipment may be borrowed:

- 10.1.1. By: Staff and Faculty or Student.
- 10.1.2. For the use of: research, instruction, presentations, and practicum use.
- 10.1.3. For the period of: 24 hours and if longer will need approval from Department Supervisor.

NOTE: BORROWING TIMES MAY BE SHORTENED AT ANY TIME IN CASE OF SIGNIFICANT DEMAND

10.2 To borrow IT equipment proper procedures must be done:

- 10.2.1. Fill out a sign-out sheet with printed name, signature, name of equipment, IU Tag Number, Serial number, model number, destination, and date.

10.3 Privileges to borrow IT equipment may be revoked or suspended due to the following:

- 10.3.1. Repeatedly returning equipment late.
- 10.3.2. Returning equipment that is damaged or otherwise not complete or in good condition.
- 10.3.3. Repeatedly not picking up booked equipment.

10.4 To book required IT equipment, visit the Computer Department.

If any assistance is needed for setting up or using the borrowed IT equipment, please contact the Computer Department.

11 ERP Data Protection Policy

11.1 PURPOSE

To ensure the security, confidentiality and appropriate use of all data processed, stored, maintained, or transmitted on Dr.BabasahebAmbedkar Open University computer systems and networks. This includes protection from unauthorized modification, destruction, or disclosure, whether intentional or accidental.

11.2 POLICY

It is the responsibility and duty of any individual who has access to University computer systems and networks to protect University data resources in whatever form, from unauthorized modification, destruction or disclosure. Without limiting the forgoing, all individuals granted access to Dr.BabasahebAmbedkar Open University Information Technology resources are expected to adhere to the following principles:

- 11.2.1. Refrain from any deliberate violation of University or departmental policy and/or any state or central law governing information privacy and use.
- 11.2.2. Refrain from attempting to access confidential or proprietary data on Dr.BabasahebAmbedkar Open University ERP and computer systems, or in any other manner, except when it is in keeping with the specific assigned duties as aDr.BabasahebAmbedkar Open University's employee.
- 11.2.3. Appropriately maintain and protect the confidentiality of any data to which access has been granted, regardless of the method used to retrieve or display it.
- 11.2.4. Refrain from making any unauthorized alterations (add/change/delete) to any data which is accessible either through legitimate granted access or any incidental access.
- 11.2.5. Refrain from remotely or physically logging into or attempting to log into another user's machine or attempt to access another user's files without the individual's permission, except when necessary in the course of performing specific assigned duties as an employee.

- 11.2.6. Refrain from attempting to compromise the security of the Dr.BabasahebAmbedkar Open University network or devices attached to the network, except when it is necessary in the course of specific assigned duties as an employee.
- 11.2.7. Insure the proper disposal of all confidential or proprietary information in whatever form in accordance with University's IT policy.

11.3 APPLICABILITY

University wide - applies to all individuals who have access to Dr.BabasahebAmbedkar Open University data, computer systems and networks, including but not limited to all Dr.BabasahebAmbedkar Open University employees and students, who may or may not have been granted access to sensitive data during the normal course of their employment with Dr.BabasahebAmbedkar Open University.

11.4 SANCTIONS

Deliberate violation of this policy will be considered as serious violation and is subject to disciplinary action, up to and including termination of the employee/student.

12 Information Disclosure Policy

12.1 Purpose:

This policy defines guidelines for making IU information public. Proper protection of this information is essential if the interests of not only IU, but also students and business partners, are to be preserved. These interests include maintenance of competitive advantage, trade secret protection and preservation of personal privacy.

12.2 Scope of Information Disclosure Policy:

- 12.2.1. All IU internal information shall be protected from unauthorized disclosure to third parties.
- 12.2.2. The disclosure of sensitive information to consultants, contractors and any third party has to be always protected by the receipt of a signed non-disclosure agreement.

12.3 Scope of Information Disclosure Policy:

- 12.3.1. Specific information about IU internal events, including new programme, staff promotions, reorganizations and information system problems will not be released to third parties.
- 12.3.2. Care will be taken to properly structure comments and questions posted to electronic bulletin boards, electronic mailing lists, and online news groups.
- 12.3.3. The staff disclosing IU internal information to third parties will be preserved markings indicating author, date, version number, usage restrictions and other details that might be useful in determining the approved usage. Policies will be enforced centrally for all constituents Institutes.

All the controversial and sensitive IU information will be released to the public in installments so that the impact of each disclosure can be measured and so that additional releases can be postponed if necessary. This is to be done with strict confidence of the Executive President and Management.

12.4 Email Disclaimer Message

This e-mail transmission may contain confidential, proprietary and/or legally privileged information and is intended only for the individual or entity named in the e-mail address. Any disclosure, copying, distribution, or reliance upon the contents of this e-mail not authorized by the sender is strictly prohibited. If you have received this e-mail transmission in error, please immediately reply to info@indusuni.ac.in to the sender, so that proper delivery of the e-mail can be effected, and then please delete the message from your Inbox. Any content of this message and its attachments that does not relate to the official business of Dr. BabasahebAmbedkar Open University or its constituent Institutes must be taken not to have been sent or endorsed by any of them. Email communications are not private and no warranty is made that e-mail communications are timely, secure or free from computer virus or other defect.

13 Intranet Policy

13.1 Purpose:

This policy defines guidelines to facilitate efficient and more effective ways for using IU's intranet facilities.

13.2 Scope of Intranet Policy

- 13.2.1. The IU's Intranet is intended exclusively for academic/official purpose.
- 13.2.2. Restriction to user to send confidential or secret information available on Intranet to external environment.
- 13.2.3. Administrators will approve all third party access to IU internal computer systems, which are not clearly public.
- 13.2.4. The IU intranet pages will have to conform to layout standards, navigation standards, and legal wording standards.
- 13.2.5. Before any computer system or network segment can be connected to IU's intranet has to get certified.

14 Intrusion Detection Policy

14.1 Purpose:

The purpose of policy is to alert information processing personnel's of IU against any intrusions to their information system.

14.2 Scope of Intrusion Detection Policy:

- 14.2.1. All the alarms and alert functions of firewalls and other network perimeter access control systems will be enabled.
- 14.2.2. User accounting, operating system and audit logging processes will be enabled.
- 14.2.3. System integrity checks of the firewalls and other network perimeter access control systems will be performed on a routine basis.
- 14.2.4. Audit logs for servers and hosts on the internal protected network will be reviewed on a weekly basis.
- 14.2.5. All trouble reports will be reviewed for symptoms that might indicate intrusive activity.

15 IT Asset Policy

15.1 Purpose:

The purpose of the policy is to bring accountability of software and hardware assets issued to the user.

15.2 Scope of IT Asset Policy:

- 15.2.1. All IT assets will be issued to the user based upon the hardware and software requirement as per the business requirement and duly approved by the HOD.
- 15.2.2. All the users will be provided hardware with standard specifications (laptop & desktop). Deviations will be subject to special approval from HOD and/or Director of the institute.
- 15.2.3. The IT assets will be issued in the name of individual user who is responsible for maintaining and upkeep of asset. User will have to fill the standard hardware requirement-cum-acknowledgement form.
- 15.2.4. HR department will provide prior information about people joining /leaving organization in advance to Computer Department.
- 15.2.5. All IT asset allocations are subject to recommendation from HOD/Director /HR.
- 15.2.6. The IT assets will be transferred to Computer Department if employees are separating from university. Re-issue of the asset will be initiated by Computer Department as per the policy.

16 IT Asset Disposal Policy

16.1 Purpose

The purpose of this policy is to establish and define standards, procedures, and restrictions for the disposal of IT equipment in a legal, cost-effective manner. Dr. BabasahebAmbedkar Open University's surplus or obsolete IT assets and resources (i.e. desktop computers, servers, databases, etc.) must be discarded according to legal requirements and environmental regulations through the appropriate external agents and Dr. BabasahebAmbedkar Open University's upgrade guidelines. Therefore, all disposal procedures for retired IT assets must adhere to University-approved methods.

16.2 Scope

This policy applies to the proper disposal of all non-leased Dr. BabasahebAmbedkar Open University IT hardware, including PCs, printers, handheld devices, servers, databases, hubs, switches, bridges, routers, and so on. University-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse are covered by this policy. Where applicable, it is desirable to achieve some residual value of the IT asset in question through reselling, auctioning, donation, or reassignment to a less-critical function.

16.3 Definitions

- 16.3.1. "Disposal" refers to the reselling, reassignment, recycling, donating, or throwing out of IT equipment through responsible, ethical, and environmentally sound means.
- 16.3.2. "Obsolete" refers to any and all equipment over 10 years old and/or that which no longer meets requisite functionality.
- 16.3.3. "Surplus" refers to hardware that has been replaced by upgraded equipment or is superfluous to existing requirements.
- 16.3.4. "Beyond reasonable repair" refers to any and all equipment whose condition requires fixing or refurbishing that is likely cost equal to or more than total replacement.

16.4 Guidelines

Disposal and disposal procedures of all IT assets and equipment will be centrally managed and coordinated by Dr. BabasahebAmbedkar Open University's Computer Department. Dr. BabasahebAmbedkar Open University's Computer Department is also responsible for backing up and then wiping clean of University data all IT assets slated for disposal, as well as the removal of University tags and/or identifying labels.

16.5 Practices

Acceptable methods for the disposal of IT assets are as follows:

- 16.5.1. Sold to existing staff.
- 16.5.2. Donated to Students.
- 16.5.3. Sold as scrap to a dealer.
- 16.5.4. Used as a trade-in against cost of replacement item.
- 16.5.5. Reassigned to a less-critical business operation function.
- 16.5.6. Donated to schools, charities, and other non-profit organizations.
- 16.5.7. Recycled and/or refurbished to leverage further use (within limits of reasonable repair).
- 16.5.8. Discarded as rubbish in a landfill after sanitized of toxic materials by approved service provider.

16.6 Policy

It is the responsibility of any employee of Dr. BabasahebAmbedkar Open University's Computer Department with the appropriate authority to ensure that IT assets, equipment, and hardware are disposed of according to one or more of the methods prescribed above. It is imperative that any disposals performed by Dr. BabasahebAmbedkar Open University are done appropriately, responsibly, and ethically, as well as with University resource planning in mind. The following rules must therefore be observed:

- 16.6.1. **Obsolete IT Assets:** As prescribed above, "obsolete" refers to any and all computer or computer-related equipment over 10 years old and/or equipment that no longer meets requisite functionality. Identifying and classifying IT assets as obsolete is the sole province of Dr. BabasahebAmbedkar Open University's

Computer Department. Decisions on this matter will be made according to Dr. BabasahebAmbedkar Open University's purchasing/procurement strategies. Equipment lifecycles are to be determined by IT asset management best practices (i.e. total cost of ownership, required upgrades, etc.).

16.6.2. **Reassignment of Retired Assets:** Reassignment of computer hardware to a less critical role is made at the sole discretion of Dr. BabasahebAmbedkar Open University's Computer Department. It is, however, the goal of Dr. BabasahebAmbedkar Open University to - whenever possible - reassign IT assets in order to achieve full return on investment (ROI) from the equipment and to minimize hardware expenditures when feasible reassignment to another business function will do instead.

16.6.3. **Trade-Ins:** Where applicable, cases in which a piece of equipment is due for replacement by a newer model, reasonable actions must be taken to ensure that a fair and market trade-in value is obtained for the old IT asset against the cost of the replacement. Dr. BabasahebAmbedkar Open University's Purchasing Head or IT Head will assume this responsibility.

16.7 Income Derived from Disposal:

Whenever possible, it is desirable to achieve some residual value from retired or surplus IT assets. Any and all receipts from the sale of IT assets must be kept and submitted to the Finance Department. Income derived from sales to staff, the public, or students must be fully receipted and amount obtained is to send to Dr.BabasahebAmbedkar Open University's Finance Department. Sales to staff should be advertised through the University intranet or via e-mail.

16.8 Assets beyond reasonable repair:

The Systems manager is responsible for verifying and classifying any IT assets beyond reasonable repair. Equipment identified as such should be kept in store as a spare for any working parts that can still be put to sufficient use within the organization. The Computer Department will inventory and

stockpile these parts. Remaining parts and/or whole machines unfit for use or any other disposal means will be sold to an approved scrap dealer.

16.9 **Decommissioning of Assets:**

All hardware slated for disposal by any means must be fully wiped clean of all University data. Dr.BabasahebAmbedkar Open University's Computer Department will assume responsibility for decommissioning this equipment by deleting all files, University-licensed programs, and applications using a pre-approved disk-sanitizer. This sanitizer must **completely overwrite** each and every disk sector of the machine with zero-filled blocks. In addition, any property tags or identifying labels must also be removed from the retired equipment.

16.10**Donations:**

IT assets with a net residual value that are not assigned for reuse, discarding, or sale to employees or external buyers, may be donated to a University-approved school, charity, or other non-profit organization (i.e. a distributor of free machines to developing nations). All donations must be authorized by Dr.BabasahebAmbedkar Open University. All donation receipts must be submitted to the Finance department for taxation purposes.

17 Network Security Policy for Portable Computers

17.1 Introduction

Portable computers offer staff the ability to be more productive while on the move. They offer greater flexibility in where and when staff can work and access information, including information on our Dr.BabasahebAmbedkar Open University network. However, network-enabled portable computers also pose the risk of data theft and unauthorized access to our Dr.BabasahebAmbedkar Open University network.

Any device that can access the Dr.BabasahebAmbedkar Open University network must be considered part of that network and therefore subject to policies intended to protect the network from harm. Any portable computer that is proposed for network connection must be approved and certified by the Computer Department.

17.2 Protecting the Laptop

In order to qualify for access to our Dr.BabasahebAmbedkar Open University network, the laptop must meet the following conditions:

- 17.2.1. Network settings, including settings for our VPN, must be reviewed and approved by Computer Department support personnel.
- 17.2.2. A personal firewall must be installed on the computer and must always be active.
- 17.2.3. Anti-virus software must be installed. Software must have active scanning and it must be kept up-to-date. Recommended anti-virus software is Microsoft Security Essential Antivirus.

17.3 Laptop User's Responsibilities

- 17.3.1. The user of the laptop is responsible for network security of the laptop whether they are onsite, at home, or on the road.
- 17.3.2. The user of the laptop is responsible for keeping their anti-virus scanning software up-to-date at all times. It is strongly

recommended that they update their anti- virus software before going on the road.

17.3.3. The user of the laptop shall access network resources via a VPN connection. Use of public Internet services is discouraged, as they do not offer adequate protection for the user.

17.3.4. The user of the laptop, whether issued by University or personally owned, must refrain from altering the hardware identity (MAC address) of the networking devices. The user found violating this policy will be subjected to disciplinary action which could lead to termination of the employee/student.

17.4 Security Audits

The Computer Department reserves the right to audit any laptop used for University activities to ensure that it continues to conform to this certification policy. The Computer Department will also deny network access to any laptop, which has not been properly configured and certified.

18 Password Security Policy

18.1 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

18.2 Scope of Password Security Policy

- 18.2.1. All the system level passwords will be as the necessity origins.
- 18.2.2. All user level passwords changes on every Three-month period for domain Network Access
- 18.2.3. Domain Administrator Login ID and Password is known to System Administrators and Manger.
- 18.2.4. We restrict all users that password must not be inserted into email messages or other form of electronic communication.
- 18.2.5. We also guided user to give screen saver and power ON password to restrict unauthorized access.
- 18.2.6. Sharing of passwords in any form is highly restricted in order to avoid unauthorized access
- 18.2.7. The users found violating this policy are subjected to disciplinary action and may lead to termination.

19 Printer Policy

19.1 Purpose

Printers represent one of the highest equipment expenditures at Dr.BabasahebAmbedkar Open University. The goal of this policy is to facilitate the appropriate and responsible academic use of Dr.BabasahebAmbedkar Open University's printer assets, as well as control Dr.BabasahebAmbedkar Open University's printer cost of ownership by preventing the waste of paper, toner, ink, and so on.

19.2 Scope

This Printer Policy applies to all employees and students of Dr.BabasahebAmbedkar Open University, as well as any contract employees in the service of Dr.BabasahebAmbedkar Open University who may be using Dr.BabasahebAmbedkar Open University networks and equipment.

19.3 Supported Printers

Dr.BabasahebAmbedkar Open University supports all network printers on the University's network Systems. An effort has been made to standardize on specific printer models in order to minimize support and recurring costs.

19.4 General Policy

- 19.4.1. Printers are to be used for documents that are relevant to the day-to-day conduct of business at Dr.BabasahebAmbedkar Open University. Dr.BabasahebAmbedkar Open University printers should not be used to print personal documents.
- 19.4.2. Installation of personal printers is generally not permitted at Dr.BabasahebAmbedkar Open University due to the cost of maintaining and supporting many dispersed machines. In certain circumstances, however, where confidentiality, remote location, the need to print a large number of low volume print jobs, or other unusual situation is an issue, personal printers could be allowed with prior permission of the HOD and HOD of Computer Department.

- 19.4.3. Do not print multiple copies of the same document - the printer is not a copier and typically costs more per page to use. If you need multiple copies, print one good copy on the printer and use the photocopier to make additional copies.
- 19.4.4. If you print something, please pick it up in a timely fashion. If you no longer want it, please dispose of it appropriately or reuse it for printing on the back side of the paper (i.e. recycle). Please be extra careful to remove old staple pins.
- 19.4.5. If you come across an unclaimed print job, please stack it neatly on the printer table. All unclaimed output jobs will be discarded at end of the day.
- 19.4.6. Make efforts to limit paper usage by taking advantage of duplex printing (i.e. double-sided printing) features offered by some printers and other optimization features (e.g. printing six PowerPoint slides per page versus only one per page).
- 19.4.7. Make efforts to limit toner use by selecting light toner and lower dpi default print settings.
- 19.4.8. Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer.
- 19.4.9. If printing a job in excess of 25 pages, please be at the printer to collect it when it comes out to ensure adequate paper supply for the job and that the output tray is not overfull (i.e. you may need to remove some of the output before the print job is finished).
- 19.4.10. Avoid printing e-mail messages. This is wasteful. Instead, use the folders and archiving functionality in your e-mail application to organize and view your messages.
- 19.4.11. Avoid printing a document just to see what it looks like.
- 19.4.12. Many printers do not support certain paper types, including vellum, transparencies, adhesive labels, tracing paper, card stock, or thicker paper. If you need to use any of the paper types, consult with Computer Department to find out which machines can handle these specialty print jobs.
- 19.4.13. Colour printing is typically not required by general users. Given this selective need, as well as the high cost per page to print

colour copies, the number of colour-capable printers available has been minimized. You are strongly encouraged to avoid printing in colour when monochrome (black) will do.

- 19.4.14. Printer paper is available to staff and students by filling requisition slip duly signed by HOD. Toner cartridges are maintained by Computer Department, any problems in print quality should be reported to Computer Department.
- 19.4.15. If you encounter a physical problem with the printer (paper jam, out of toner, etc.) and are not "trained" in how to fix the problem, please do not try. Instead, report the problem to Computer Department for help.
- 19.4.16. Report any malfunction of any printing device to the Computer Department as soon as possible on ext. 2014 or by email systemdept@indusuni.ac.in or on intranet Helpdesk.

20 Removable Media Acceptable Use Policy

20.1 Scope

The policy applies to any hardware and related software that could be used to access or our organization resources, even if said equipment is not corporately sanctioned, owned, or supplied.

20.2 Usage

The overriding goal of this policy is to protect the integrity of the private and confidential data that resides within Dr.BabasahebAmbedkar Open University's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently moved outside the enterprise network and/or the physical premises where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of information, damage to critical applications, loss of revenue, and damage to the university's public image. Therefore, all users employing removable media and/or USB-based technology to backup, store, and otherwise access corporate data of any type must adhere to company-defined processes for doing so.

- 20.2.1. Portable USB-based memory sticks, also known as flash drives, or thumb drives, jump drives, or key drives.
- 20.2.2. Memory cards in SD, CompactFlash, Memory Stick, or any related flash-based supplemental storage media.
- 20.2.3. USB card readers that allow connectivity to a PC.
- 20.2.4. Portable MP3 and MPEG-playing music and media player-type devices such as iPods with internal flash or hard drive-based memory that support data storage function.
- 20.2.5. PDAs, cell phone handsets, and smartphones with internal flash or hard drive-based memory that support data storage function.
- 20.2.6. Digital cameras with internal or external memory support.
- 20.2.7. Removable memory-based media, such as rewritable DVDs, CDs, and floppy disks.
- 20.2.8. Any hardware that provides connectivity to USB devices through means such as wireless (WiFi,WiMAX, irDA, Bluetooth, among others) or wired network access.

20.3 Applicability

This policy applies to all DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY employees, including full and part-time staff, contractors, freelancers, and other agents, who utilize either company-owned or personally-owned removable media and/or USB-based technology to store, back up, relocate or access any organization or client-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY has built with its clients, supply chain partners and other constituents. Consequently, employment at Dr.BabasahebAmbedkar Open University does not automatically guarantee the initial and on-going ability to use these devices within the enterprise technology environment.

It addresses a range of threats to - or related to the use of - enterprise data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright	Software copied onto portable memory device could violate licensing.
Spyware	Spyware or tracking code enters the network via memory media.
Malware	Viruses, Trojans, Worms, and other threats could be introduced via external media.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the enterprise to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional USB-related connectivity within corporate facilities will be managed at the sole discretion of Computer Department. Non-sanctioned use of USB-based hardware, software, and/or related components to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of portable memory devices to any element of the enterprise network.

20.4 Affected Technology

All USB-based devices and the USB ports used to access workstations and other related connectivity points within the corporate firewall will be centrally managed by DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department and will utilize encryption and strong authentication measures. Although Computer Department is not able to manage the external devices - such as home PCs - to which these memory resources will also be connected, end users are expected to adhere to the same security protocols when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

20.5 Policy and Appropriate Use

It is the responsibility of any employee of DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY who is connecting a USB-based memory device to the organizational network to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any portable memory that is used to conduct Dr. Babasaheb Ambedkar Open University day to day activities is utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

20.6 Access Control

- 20.6.1. Computer Department reserves the right to refuse, by physical and non-physical means, the ability to connect removable media and USB devices to corporate and corporate-connected infrastructure. **Computer Department will engage in such action if it feels such equipment is being used in such a way that puts the university's systems, data, users, and clients at risk.**

- 20.6.2. Prior to initial use on the corporate network or related infrastructure, all USB-related hardware and related software must be registered with Computer Department. A list of approved USB devices and related software is available for viewing at feature not available yet. If your preferred device does not appear on this list, contact the help desk. Although Computer Department currently allows only listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in future.
- 20.6.3. End users who wish to connect such devices, to non-corporate network infrastructure, to gain access, to enterprise data must employ, for their devices and related infrastructure, a company-approved personal firewall and any other security measure deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's established enterprise IT security standards.
- 20.6.4. DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY will maintain a list of approved USB-based memory devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure.

20.7 Security

Employees using removable media and USB-related devices and related software for data storage, back up, transfer, or any other action within DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's technology infrastructure will, without exception, use secure data management procedures. A simple password is insufficient. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

- 20.7.1. All USB-based devices that are used for business interests must be pre-approved by Computer Department, and must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not

they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain enterprise data. Any non--corporate computers used to synchronize with these devices will be installed whatever anti-virus and anti-malware software deemed necessary by DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department. Antivirus signature files on any additional client machines - such as a home PC - on which this media will be used, must be updated in accordance with existing company policy.

- 20.7.2. All removable media will be subject to quarantine upon return to the office before they can be fully utilized on enterprise infrastructure.
- 20.7.3. Passwords and other confidential data as defined by DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department are not to be stored on portable storage devices.
- 20.7.4. End users must apply new passwords for every business/personal trip where company data is being utilized on USB-based memory devices.
- 20.7.5. Any USB-based memory device that is being used to store DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY data must adhere to the authentication requirements of DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department. In addition, all hardware security configurations (personal or company-owned) must be pre-approved by DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department before any enterprise data-carrying memory can be connected to it.
- 20.7.6. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase company-specific data from such devices once their use is no longer required. See sanitation policy for detailed data wipe procedures for flash memory.

20.8 Help & Support

- 20.8.1. DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media. This applies even to devices already known to the IT department.
- 20.8.2. Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department. This includes, but is not limited to, reconfiguration of USB ports.
- 20.8.3. Computer Department may restrict the use of Universal Plug and Play on any client PCs that it deems to be particularly sensitive. Computer Department also reserves the right to disable this feature on PCs used by employees in specific roles.
- 20.8.4. Computer Department reserves the right to summarily ban the use of these devices at any time. Computer Department need not provide a reason for doing so, as protection of confidential data is the highest and only priority.
- 20.8.5. Computer Department reserves the right to physically disable USB ports to limit physical and virtual access.
- 20.8.6. Computer Department reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

20.9 Organizational Protocol

Computer Department can and will establish audit trails in all situations it feels merited. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order

to identify accounts/computers that may have been compromised by external parties. In all cases, data protection remains DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's highest priority.

- 20.9.1. The end user agrees to immediately report to his/her manager and DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY's Computer Department for any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of company resources, databases, networks, etc.
- 20.9.2. DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY will not reimburse employees if they choose to purchase their own USB-based memory devices.
- 20.9.3. Any questions relating to this policy should be directed to Computer Department.

20.10 Policy Non-Compliance

Failure to comply with the Removable Media and Acceptable Use Policy may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

21 Reporting Critical Service Outages During Academic Term

During normal operating hours (Monday - Saturday, 8:50 a.m. - 5:00 p.m.), members of the University community should notify the Computer Department of suspected problems with computers, networks, and related information technology resources. Computer Department will investigate the problem and determine corrective action. If the Computer Department staff determines that the problem is related to the campus network or a server, they will notify Computer Department Manager who will take appropriate action. Resolution of critical service outages (defined below) will be a top Computer Department priority and will be resolved in a timely manner. Non-critical problems will be investigated and resolved as soon as is feasible.

Outside of operating hours and on University holidays suspected critical service outages should be reported as follows:

5:00 p.m. - 10 p.m. (Monday - Saturday) and 10 a.m. - 10 p.m., Saturday and Sunday.

Any suspected critical service outages should be reported to the Computer Department personnel on duty in the Dr. Babasaheb Ambedkar Open University. The student will follow prescribed diagnostic routines to determine if the problem is indeed of a critical nature. If so, he/she will call the appropriate Computer Department staff member to resolve the problem. No member of the community should call Computer Department staff outside of normal operating hours.

Outside of these times, suspected critical service outages should be reported at the next designated time the following day.

21.1

A critical service outage is defined as one or more of the following:

- 21.1.1. Failure of the campus network equipment or Internet connection making it impossible for a majority of users to access on campus or off campus resources.

- 21.1.2. Campus wide printing failure (not individual printers).
- 21.1.3. Failure of a majority of computers in a computer lab.
- 21.1.4. Failure of the authenticating server affecting the entire campus.
- 21.1.5. Failure of the University Domain System affecting the entire campus.
- 21.1.6. Failure of the University Email Systems affecting the entire campus.
- 21.1.7. Failure of the University ERP Systems affecting the entire campus.

22 Server Security Policy

22.1 Purpose:

The purpose of this policy is to establish standards for the base configuration of IU servers used for information processing functions. Effective implementation of this policy will minimize unauthorized access to IU proprietary information and technology.

22.2 Scope of Secure Policy:

- 22.2.1. All servers are taken care of by the system administrator for their security on day-to-day basis.
- 22.2.2. The recommended security settings in different OS will be specified in the configuration of the servers.
- 22.2.3. The unnecessary services in the OS are disabled as laid out in configuration guide.
- 22.2.4. Physical and logical securities are taken care of for restricting unauthorized access.
- 22.2.5. System administrator sets password for power ON for adding security points.
- 22.2.6. All passwords are written in sheet of a paper which is in custody of System Administrator/Manager.

23 Software Licensing Policy

23.1 Purpose:

The purpose of this policy is to provide guidelines for licensed software use on IU information resources. These guidelines are necessary to prevent IU from violating any software licensing law.

23.2 Scope of Secure Policy:

- 23.2.1. IU will ensure that sufficient licensed copies of software, Operating Systems so that information processing personnel can get their work done in expedient and effective manner.
- 23.2.2. Third party copyrighted information or software; that IU does not have specific approval to store and/or use will not be stored on IU system networks.
- 23.2.3. Third party software in the possession of IU will not be copied unless such copying is consistent with relevant license agreements and prior management approval.
- 23.2.4. The users must refrain from installing/using the software which is not licensed by IU.
- 23.2.5. The users found violating this policy are subjected to disciplinary action and may lead to termination.

24 Tablets/Smartphone Usage Policy

24.1 Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Dr.BabasahebAmbedkar Open University's internal network(s) or related technology resources via any means involving mobile devices that are categorized as Personal Digital Assistants (Smartphones)/Tablets/Smart Phone hereafter referred as Smartphone. This policy applies to, but is not limited to, all devices that fit the following device classifications:

- 24.1.1. Tablets / Smartphones running IOS, Android, Windows Mobile OS, Blackberry OS, Mobile Linux Operating Systems etc.
- 24.1.2. Handhelds running the Android, IOS, Microsoft Windows CE, Pocket-PC or Windows Mobile, Symbian, or Mobile Linux Operating Systems.
- 24.1.3. Mobile devices that are standalone (i.e. connectible using wired sync cables and/or cradles.)
- 24.1.4. Devices that have integrated wireless capability. This capability may include, but is not limited to, Wi-Fi, Bluetooth, and IR.
- 24.1.5. Phone/Tablets that include Smartphone functionality.
- 24.1.6. Any related components of Dr.BabasahebAmbedkar Open University's technology infrastructure used to provide connectivity to the above.
- 24.1.7. Any third-party hardware, software, processes, or services used to provide connectivity to the above.

The policy applies to any Smartphone hardware and related software that could be used to access Dr.BabasahebAmbedkar Open University resources, even if said equipment is not Dr.BabasahebAmbedkar Open University's sanctioned, owned, or supplied.

The overriding goal of this policy is to protect Dr.BabasahebAmbedkar Open University's technology-based resources (such as Dr.BabasahebAmbedkar Open University data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public

image. Therefore, all users employing Smartphone-based technology to access Dr.BabasahebAmbedkar Open University technology resources must adhere to University-defined processes for doing so.

24.2 Scope

24.2.1. This policy applies to all Dr.BabasahebAmbedkar Open University employees, including full-time and part-time staff, contractors, freelancers, and other agents who utilize University-owned, personally owned, or publicly-accessible Smartphone-based technology to access the organization's data and networks via wired and wireless means. Such access to enterprise network resources is a privilege, not a right. Consequently, employment at Dr.BabasahebAmbedkar Open University does not automatically guarantee the granting of these privileges.

24.2.2. Addition of new hardware, software, and/or related components to provide additional Smartphone-related connectivity within Dr.BabasahebAmbedkar Open University facilities will be managed at the sole discretion of Computer Department and prior approval of competent authority. Non-sanctioned installations of Smartphone-related hardware, software, and/or related components, or use of same within the organizational campus, or to gain access to organizational computing resources, are strictly forbidden.

24.2.3. This policy is complementary to any previously implemented policies dealing specifically with network access, wireless access, and remote access to the enterprise network.

24.3 Supported Technology

All Smartphones and related connectivity points within the Dr.BabasahebAmbedkar Open University firewall will be centrally managed by Dr.BabasahebAmbedkar Open University's Computer Department and will utilize encryption and strong authentication measures. Although Computer Department is not able to manage the public network to which wireless-enabled Smartphone devices and smartphones initially connect, end- users are expected to adhere to

the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the University's infrastructure.

The following table outlines Dr.BabasahebAmbedkar Open University's minimum Systems requirements for a computer, workstation, or related device to properly support and sustain Smartphone connectivity and functionality. Equipment that does not currently meet these minimum requirements will need to be upgraded before Smartphone implementation may be sanctioned by Computer Department.

24.4 Eligible Users

All employees requiring the use of Smartphones for official purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. Application forms must be approved and signed by the employee's Department Head, Director, before submission to the Computer Department.

Employees may use privately owned Smartphones (under 'Supported Technology') for official purposes. If this is the case, the Computer Department must approve the specific handheld and connection type as being secured and protected. However, the University's Computer Department cannot and will not technically support third-party wireless hardware or software, or any other unapproved remote e-mail connectivity solution.

24.5 Policy and Appropriate Use

24.5.1. It is the responsibility of any employee of Dr.BabasahebAmbedkar Open University who is connecting to the organizational network via a Smartphone to ensure that all components of his/her connection remain as secure as his/her network access within the office. It is imperative that any wired (via sync cord, for example) or wireless connection, including, but not limited to Smartphone devices and service, used to conduct Dr.BabasahebAmbedkar Open University official to be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- 24.8.1.1. Employees using Smartphones and related software to connect to Dr.BabasahebAmbedkar Open University's technology infrastructure will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Dr.BabasahebAmbedkar Open University's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if official work is conducted from home.
- 24.8.1.2. All Smartphones that are used for official interests, whether personal- or University-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-Dr.BabasahebAmbedkar Open University computers used to synchronize with Smartphones will have installed whatever antivirus software deemed necessary by Dr.BabasahebAmbedkar Open University's Computer Department. Antivirus signature files must be updated in accordance with existing University policy.
- 24.8.2. Passwords and other confidential data as defined by Dr.BabasahebAmbedkar Open University's IT Department are not to be stored on Smartphones or their associated storage devices (such as SD and CF cards, as well as Memory Sticks and related flash-based supplemental storage media.)
- 24.8.3. Due to the potential for bandwidth conflicts within the Dr.BabasahebAmbedkar Open University campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have need to use such equipment - for example, a wireless Smartphone or smartphone - please consult Computer Department before proceeding further.

- 24.8.4. Prior to initial use for connecting to the Dr.BabasahebAmbedkar Open University network, all Smartphone- related hardware, software and related services must be registered with Computer Department. If your preferred Smartphone solution does not appear on this list, contact the Computer Department to have it registered and added to the list.
- 24.8.5. Remote users using non-Dr.BabasahebAmbedkar Open University network infrastructure to gain access to Dr.BabasahebAmbedkar Open University resources via their Smartphones must employ for their devices and related infrastructure a University-approved personal firewall, VPN, and any other security measure deemed necessary by the Computer Department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Dr.BabasahebAmbedkar Open University's additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.
- 24.8.6. Any Smartphone that is configured to access Dr.BabasahebAmbedkar Open University resources via wireless or wired connectivity must adhere to the authentication requirements of Dr.BabasahebAmbedkar Open University's Computer Department. In addition, all hardware security configurations (personal or University-owned) must be approved by Dr.BabasahebAmbedkar Open University's Computer Department.
- 24.8.7. Employees, contractors, and temporary staff will make no modifications of any kind to University-owned and installed hardware or software without the express approval of Dr.BabasahebAmbedkar Open University's Computer Department. This includes, but is not limited to, installation of Smartphone software on University-owned desktop or laptop computers, connection of sync cables and cradles to University-

owned equipment, and use of University-owned wireless network bandwidth via these devices.

- 24.8.8. Dr.BabasahebAmbedkar Open University will maintain a list of approved Smartphone-specific software applications and utilities.
- 24.8.9. Employees, contractors, and temporary staff with Dr.BabasahebAmbedkar Open Universitysanctioned wireless-enabled Smartphones must ensure that their computers and handheld devices are not connected to any other network while connected to Dr.BabasahebAmbedkar Open University's network via remote access.
- 24.8.10. All connections that make use of wireless Smartphone access must include a "time-out" Systems. In accordance with Dr.BabasahebAmbedkar Open University's security policies, sessions will time out after 30 minutes of inactivity, and will terminate after 8 hours of continuous connection. Both time-outs will require the user to reconnect and re- authenticate in order to re-enter University networks through a wireless Smartphone connection.
- 24.8.11. The Smartphone-based user agrees to immediately report to his/her manager and Dr.BabasahebAmbedkar Open University's Computer Department any incident or suspected incidents of unauthorized access and/or disclosure of University resources, databases, networks, etc.
- 24.8.12. The Smartphone-based wireless access user also agrees to and accepts that his or her access and/or connection to Dr.BabasahebAmbedkar Open University's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

24.8.13. Dr.BabasahebAmbedkar Open University will not reimburse employees for official-related wireless Smartphone-based access connections made on a pre-approved privately owned ISP service. All submissions for reimbursement must be accompanied by sufficient and appropriate documentation (i.e. original service bill). Employees requesting reimbursement will also be asked to certify in writing prior to reimbursement that they did not use the connection in any way that violates University policy.

24.8.14. IT reserves the right to turn off without notice any access port to the network that puts the University's systems, data, users, and clients at risk.

24.6 Policy Non-Compliance

Failure to comply with the Smartphone Usage Policy and Agreement may, at the full discretion of the organization, result in the suspension of any or all-remote access privileges, disciplinary action, and possibly termination of employment

25 Wireless Security Access Policy

25.1 Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Dr.BabasahebAmbedkar Open University's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- 25.1.1. External hosts via remote access technology (for example, using a wireless router at home to connect to the Dr.BabasahebAmbedkar Open University Virtual Private Network).
- 25.1.2. Wireless gateways on Dr.BabasahebAmbedkar Open University premises.
- 25.1.3. Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access Dr.BabasahebAmbedkar Open University resources, even if said equipment is not Dr.BabasahebAmbedkar Open University owned, or supplied. For example, use of a personal laptop / computer / smartphone either from outside or within campus to access the Dr.BabasahebAmbedkar Open University network would fall under the scope of this policy.

The basic aim of this policy is to protect Dr.BabasahebAmbedkar Open University's technology-based resources (such as Dr.BabasahebAmbedkar Open University data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing Dr.BabasahebAmbedkar Open University technology resources must adhere to University-defined processes for doing so.

25.2 Scope

- 25.2.1. This policy applies to all Dr.BabasahebAmbedkar Open University employees, including full-time staff, part-time staff, students, contractors, freelancers, and other agents who utilize University-

owned, personally-owned, or publicly-accessible computers to access the organization's data and networks via wireless means. Wireless access to enterprise network resources is a privilege, not a right. Consequently, employment at Dr.BabasahebAmbedkar Open University does not automatically guarantee the granting of wireless access privileges.

25.2.2. Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general-purpose access in areas of transient use, such as common areas and selected classrooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

25.2.3. Addition of new wireless access points within Dr.BabasahebAmbedkar Open University facilities will be managed at the sole discretion of Computer Department. Non-sanctioned installations of wireless equipment, or use of unauthorized equipment within the organizational campus, are strictly forbidden. This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the enterprise network.

25.3 Supported Technology

All wireless access points within the Dr.BabasahebAmbedkar Open University firewall will be centrally managed by Dr.BabasahebAmbedkar Open University's IT Department and will utilize encryption, strong authentication, and other security methods at Computer Department's discretion. Although Computer Department is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the University's infrastructure.

25.4 Eligible Users

All employees requiring the use of wireless access for business purposes must go through an application process that clearly outlines why the access is required and what level of service the employee needs should his/her application be accepted. Computer Department will define a list of traffic types that are acceptable for use over a wireless connection. More sensitive business activities will be similarly defined, and will be limited to non-wireless environments. Application forms must be approved and signed by the employee's department head before submission to the Computer Department. Employees may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, the Computer Department must approve the wireless connection as being secure and protected. However, the University's Computer Department cannot and will not technically support third-party wireless hardware or software, a hotspot wireless ISP connection, or any other wireless resource located outside the Dr.BabasahebAmbedkar Open University firewall. In the event that expenses are incurred and management has approved reimbursement, all expense forms for reimbursement of costs (if any) incurred due to the need for wireless access for official purposes (i.e. Internet connectivity charges) must be submitted to the appropriate unit or department head. Financial reimbursement for wireless access is not the responsibility of the Computer Department. If you foresee an upcoming need for this class of access, ask your section head to help you fill out a proposal.

25.5 Policy and Appropriate Use

It is the responsibility of any employee of Dr.BabasahebAmbedkar Open University who is connecting to the organizational network via wireless means to ensure that all components of his/her wireless connection remain as secure as his or her network access within the office. It is imperative that any wireless connection used to conduct Dr.BabasahebAmbedkar Open University business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

- 25.5.1. General access to the organizational network through the Internet by residential remote users through Dr.BabasahebAmbedkar Open University's network is restricted. However, an employee can access the organizational network with prior permission of Head of

- the Department in conjunction with Computer Department. No student will be allowed to access organizational network through Internet.
- 25.5.2. Employees using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Dr.BabasahebAmbedkar Open University's password policy. Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.
 - 25.5.3. All remote computer equipment and devices used for business interests, whether personal or University-owned, must display reasonable physical security measures. Users are expected to secure their Dr.BabasahebAmbedkar Open University-connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by Dr.BabasahebAmbedkar Open University's IT Department. Antivirus signature files must be updated in accordance with existing University policy.
 - 25.5.4. Prior to initial use for connecting to the Dr.BabasahebAmbedkar Open University network, all public hotspots must be registered with Computer Department.
 - 25.5.5. Any remote connection that is configured to access Dr.BabasahebAmbedkar Open University resources must adhere to the authentication requirements of Dr.BabasahebAmbedkar Open University's Computer Department. In addition, all hardware security configurations (personal or University-owned) must be approved by Dr.BabasahebAmbedkar Open University's Computer Department.
 - 25.5.6. Employees, contractors, and temporary staff will make no modifications of any kind to University-owned and installed wireless

hardware or software without the express approval of Dr.BabasahebAmbedkar Open University's Computer Department.

- 25.5.7. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to Dr.BabasahebAmbedkar Open University's network via remote access.
- 25.5.8. The wireless access user agrees to immediately report to his/her manager and Dr.BabasahebAmbedkar Open University's IT Department any incident or suspected incidents of unauthorized access and/or disclosure of University resources, databases, networks, and any other related components of the University's technology infrastructure.
- 25.5.9. The wireless access user also agrees to and accepts that his or her access and/or connection to Dr.BabasahebAmbedkar Open University's networks may be monitored to record dates, times, duration of access, data types and volumes, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
- 25.5.10. System Department reserves the right to turn off without notice any access port to the network that puts the University's systems, data, users, and clients at risk.
- 25.5.11. Failure to comply with the Wireless Security Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employee.