Information Technology (IT) Governance Policy

Babu Banarasi Das University

BBD City, Ayodhya Road, Lucknow 226 028
Uttar Pradesh, India
www.bbdu.ac.in

Scope

The policy is defined to broadly cover all the stakeholders on campus or off campus inclusive of University faculty, Administrative staff, Higher Authorities, Students, Guests and all others using the IT resources, whether personally or of University owned.

Objective

University IT policy exists to maintain, secure and ensure legal and appropriate use of Information technology infrastructure established by the University for promoting the mission of the University towards teaching, learning, research and administration. This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, Reliability and Availability of the information assets that are accessed, created, managed, and/or controlled by the University. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

IT & Hardware Asset Management

The University shall lay down business processes for the management of IT & Hardware assets.

A. Primary User - An individual in whose room / work station the computer is installed and is primarily used by him/her is considered to be "primary" user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. End User Computer Systems - Apart from the client PCs used by the users, the university will consider servers not directly administered by INTERNET UNIT, as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the INTERNET UNIT, are still considered under this policy as "end users" computers.

C. Warranty & Annual Maintenance Contract - Computers purchased by any Section/Department/Project should preferably be with 3-year onsite comprehensive warranty.

After the expiry of warranty, the Computer Centre shall maintain all systems. Such maintenance should include OS re-installation and checking virus related problems also.

D. Power Supply to Computers and Peripherals - All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

E. Network Cable Connection - While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing - File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Shifting of Computer from One Location to another - Computer system may be moved from one location to another with prior approval and Computer Centre should be intimation to to maintain a record of computer identification names and corresponding IP address.

H. Maintenance - For all the computers that were purchased by the university centrally, the Computer Centre will attend the complaints related to any maintenance related problems.

I. Noncompliance - BBDU faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's noncompliant computer can have significant, adverse effect on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

Software Management

Any computer purchases made by the individual departments/projects should make sure that such computer systems have all software (operating system, antivirus software and necessary application software) installed.

A. Operating System and its Updating

1. Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through Internet. Updating OS by the users helps their computers in fixing bugs. Checking for updates and updating of the OS should be performed at least once in a week or so.

2. University as a policy encourages user community to go for open source software such as Linux, Open office to be used on their systems wherever possible.

Data Base Management

BBDU databases are maintained by the University's System Administration. Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. BBDU has its own policies regarding the creation of database and access to information.

A. Database Ownership: Babu Banarasi Das University is the data owner of all the University's institutional data generated in the university.

B. Custodians of Data: Individual Sections or departments generate portions of data that constitute University's database. They may have custodianship responsibilities for portions of that data.

C. Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

Uninterrupted Power Supply (UPS)

All servers, desktops and peripherals (excluding laptops, Ipads) should be connected through an Uninterrupted power supply (UPS) unit for smooth functioning during brief power cuts and also protection of equipment during power surges. Power supply to the UPS should maintain adequately to ensure regular battery charging. In this regard the user/Head may coordinate with the University System Administration to ensure the same.

Data Backup

BBDU System Administration is responsible for ensuring that critical servers, data are well protected and preserved against loss & destruction. Here is our little policy for Data Backup & Restore:

Each critical Server will be backed up on regular basis.

Copies of all backup data should be stored at a secure, off -site location

Backups should not be stored in the same building as the live data or system.

Backup & Restore processes must be tested frequently.

Data compression algorithms should be used to minimize the data volume.

Website Management

Web Site Hosting Policy

Official Web pages must conform to the University's IT Cell Creation Guidelines for Web site hosting. As on date, the university's Webcell is responsible for maintaining the official web site of the university viz., http://www.bbdu.ac.in

Official Email Service

Mailing system Setup

1. Babu Banarasi Das University is having registered domain bbdu.ac.in.
2. The mail Server can be access from outside, for sending and receiving the Emails, on behalf of Babu Banarasi Das University, these email servers are being maintained by an external agency named Google Work space (G-suite) for Education. and by IT Cell, all administration of emails is done using its Web interface.
3. All Email servers are well equipped with facility of antivirus protection, Spam emails filtering.

Process and policies of using Mailing system

1. Users can send and receive a mail up to a maximum of 25 MB in size.
2. Quota Size will be 30 GB as a Standard, size can be increased based on the requirement of Process owner and preferably with the approval of Dean (Verbal / written).
3. The Mail server should not be used to transmit materials of threatening nature, including threats of death or physical harm, harassment, libel, and defamation.

REGISTRAR
BBD UNIVERSITY
LUCKNOW

4. The Mail server may not be used for the distribution of offensive materials, including obscene pornographic, indecent and hateful materials. Sending any unsolicited email that could be expected, in Sahara IP discretion, to provoke complaints. Sending email with charity requests, petitions for signatures, or any chain mail related materials, sending of Pictures and movies for the purpose of joy and entertainment. Users found doing the same shall be questioned and there id will be blocked.
5. All the emails passing the mail servers are being scanned for viruses and if found infected by virus shall be dropped; System Administration Support in no case can recover any such dropped email.
6. BBDU HR will have to request for email id creation of new employees and when the user leaves the organization his / her email id is retained or deleted as per the instructions the concerned Department/Office.
7. Users can request for the change of the email password by forwarding their request to IT Cell.
8. Email ID once made shall not be requested for modification.

Antivirus policy

1. All computers (clients and servers) connected to the organization computer network or networked resources shall have antivirus software (the most current version) correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.
2. If deemed necessary to prevent viral propagation to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code shall be disconnected from the network until the infection has been removed.

   If a computer does not have antivirus software installed, it shall be immediately informed to System Administration Support for the installation.
3. No user is allowed to disable the virus check program and shall ensure all systems under his/ her control are updated with latest signatures.
4. It shall be responsibility of the user to ensure that their system is updated with latest antivirus update.
5. Other operating systems or computing platforms shall have comparable protection, If available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all

prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

6. Use of any kind of hard disc/CD from outside is not allowed in the organization if in any case it is to be used in the organization for specific project usage by the proper approval from HOD and System Administration Support, it is first scan for viruses. And if found virus frees, then only can be used in the machines and network.

Internet

1. Internet access facility has been provided to each user/at Babu Banarsi Das University.
2. Use of Internet is only allowed for official usage.
3. Use of internet is not allowed for:-

- Unauthorized access to or use of data, systems or networks including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of system or network
- Getting online news updates, listening online music, seeing online movies, downloading pictures, screen shots wallpapers, songs, and material not useful for official usage.
- Surfing to restricted sites (blocked at proxy server) through some other means is strictly not allowed.
- Uploading/downloading data to/from to free space-providing sites on the Internet is strictly not allowed.
- Using chat and messenger on for communication within and from outside world in not allowed, the same could only be provided on specific project request after getting proper approval.

4. Faster Internet access can be provided to individual user subject to project requirement for same proper approval on email from Dean along with time period, name and IP address of machine has to be provided to System Administration Support.
5. Use of Internet for taking out any Intellectual Property of Babu Banarasi Das University by any method is a criminal offence.

Password Policy

1. All the University servers like mail, ERP are not directly accessible to users. Users can only use their services but cannot directly login into these servers for any kind of access.
2. Passwords of these servers are maintained by System Administration only and these passwords are changed periodically. No soft copy of this sheet is maintained only hard copy remains with System Administration.
3. The project servers which are controlled by System Administration Support, their administrator password is also maintained by System Administration and they are also changed periodically.
4. In case if the administrator password requirement to user is mandatory then System Administration Support can only provide the password on written approval from VC / Dean specifying the time of requirement. Also System Administrator shall not be providing the actual password to user the password shall be changed and then provided and when the job is over the original password shall be restored.

Security

The University IT resources shall not be used for activities violating the basic functionality and mission of the University.

The users must refrain from making any unauthorised access of information in order to promote secure access of network and computers.

The competent system administrator may access the information resources for a legitimate maintenance purpose.

Antivirus and security updates - The regular updating of the anti-virus policy and security updates should be done for the protection of computing resources.

Maintenance

Lab systems are maintained by Lab assistant.

Primary level problems are taken care by Lab assistant, such as power connections, Hardware troubleshooting, Booting problem, Network problem, Software installation / uninstallation, Hardware replacement, Clearing the junks & cache.

Major Network, software and Operating system related problems are taken care by System **Administrator.**

Support Hours

1. **Support shall be available on all working** days between 09:00 AM to 5:30 PM.
2. **After office hours support (Up to 8:00PM)** will be available on only written request to **System Administrator, having proper approval** of Dean/Head.
3. **Any kind of support on Sunday's, off** days or late hours have to be pre informed to **System Administrator in three days advance** with proper approval from VC, Dean & **Head specifying the timings of the support**.

REGISTRAR
BBD UNIVERSITY
LUCKNOW