Bharati Vidyapeeth
(Deemed to be University), Pune

A+ Accreditation (third cycle) by NAAC in 2017
Category-I Deemed to be University Grade by UGC
68th Rank among Universities by NIRF-2021

Information Technology Policy (ICT Policy) – Revised 2021

Bharati Vidyapeeth (Deemed to be University), Pune
Bharati Vidyapeeth Bhavan
Lal Bahadur Shastri Marg, Pune – 411030 (India)

Contents

Bharati Vidyapeeth (Deemed to be University), Pune (India)

Preface

We at BharatiVidyapeeth (Deemed to be University), Pune realising the critical role of Information and Communication Technology (ICT) in higher education, are committed to the application of ICT for enhancing administrative efficiency and to optimise learning experiences. The University ICT Policy states that:

- Access, economy, efficiency, effectiveness, relevance, transparency, privacy, accountability, sustainability, learner-centred, pedagogically driven and quality assurance shall be the guiding principles of the ICT Policy.
- The ICT applications cover the areas like system management, research, teaching and learning, student evaluation, support services, community engagement, student data management, human resource development networking and quality assurance.
- As an ongoing process, ICT applications shall take note of the rapid pace of technology changes.
- ICT policy management shall be integrated with the overall institutional development plan of the university.
- ICT system management must ensure integrity, security and legitimate applications of ICT.
- Use ICT effectively for building national and international networks to ensure innovative changes in providing quality education.
- The University shall take appropriate measures for the capacity building of academic, administrative and professional staff to effectively use ICT in all university operations.

# Preface

1: The University Context

Established in 1996, Bharati Vidyapeeth (Deemed to be University), Pune has 29 constituent institutions spread over on eight campuses located in Pune, New Delhi, Navi Mumbai, Kolhapur, Sangli, Karad and Solapur. The University offers more than 300 academic programmes, in 12 faculties - medicine, dentistry, ayurved, homoeopathy, nursing and pharmacy; engineering and technology; management; law ; science; arts, commerce and social sciences; and interdisciplinary studies, besides doctoral programme in 77 subjects A distinctive feature of the University is that it has three self-financing research institutes which conduct research on socially relevant topics and emerging areas in Health Sciences, Pharmaceutical Sciences and Social Sciences. The University's academic and research excellence has been appreciated and endorsed by different apex authorities. The Ministry of Human Resource Development, Government of India has awarded "A" grade status to the University, while NAAC has accredited it with "A+" grade (third cycle). The University is one of the few deemed universities which have earned the distinction of being recognized under Section 12(B) of UGC Act, 1956. Various academic programmes in the colleges of Pharmacy, Engineering and Management are also accredited by the National Board of Accreditation.

Its mission being Social Transformation through Dynamic Education, the University is continuously reengineering its academic and administrative processes so as to make them student centered and student friendly – by deploying the latest ICT tools. The University's ICT infrastructure is huge which includes thousands of computers, minimum 40+ Mbps internet connectivity for individual constituent units, wi-fi connectivity in all institutions, latest general and discipline specific software and video-conferencing facilities. The University has also been connected to National Knowledge Network (NKN) of the National Mission on Education through ICT (NMEICT) through one GBPS bandwidth network.

The University has its own ICT Center to develop, deploy and maintain a world-class ICT infrastructure and information resources, and to facilitate the effective use of the technology in all academic and administrative processes. Accordingly, the ICT Center established by the university aims at enhancing the Quality of the products and processes of the University by providing exhaustive and efficient ICT services to its stake holders. University's constituent units are interconnected, and together are connected to University's own Data Center.

2: Introduction

Information and Communication Technology (ICT) is an umbrella term that encompasses various communication technologies such as internet and other digital media which facilitate access to information and knowledge. The Information and Communication Technology Policy (ICT Policy) is an expression of broad intent and plan of action to putting ICT to use effectively in all university activities. The University is committed and deeply engaged in the application of ICT to enhance administrative efficiency to optimise learning experiences and to innovate. The ICT Policy framework will help the University in activities like strategic planning, change management and learning process development.
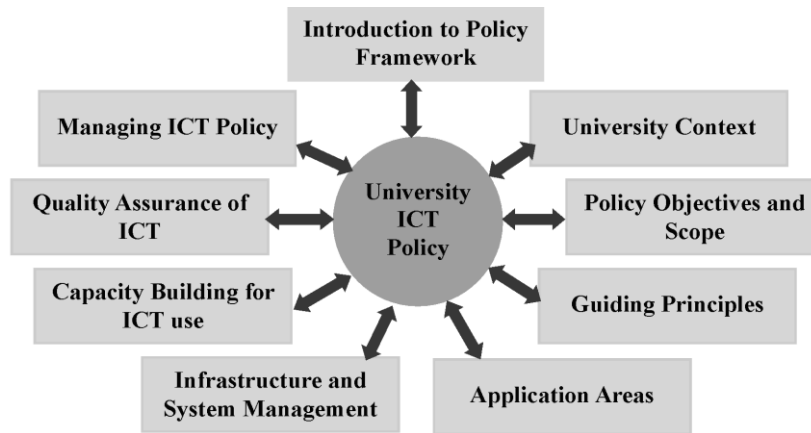
Policy Framework for ICT Applications

3: Objectives of ICT Policy

- Make the University more accessible to the present and prospective stakeholders and empowering them through enhanced access to information and quality services while improving governance through the use of ICT.
- Facilitate effective communication for the learning enrichment and student engagement.
- Develop international linkages with a view to facilitate participation in national, regional and international networks strengthening teaching, learning and research in the University.
- Create employment opportunities for the youth and improve their employability through ICT based educational initiatives and industry focused curricula and to help them participate in the ICT revolution, derive economic benefits and eventually become self-reliant.
- Promote and strengthen new Information Technology Enabled Services (ITES) / Information Technology (IT) destinations across the University by providing assistance in setting up quality IT infrastructure.
- Create world class ICT infrastructure for seamlessly connecting and integrating all ICT Service Providers and End Users.
- Use appropriate technological systems to improve communication and interaction between University office and its Constituent Institutions.

4: Scope of ICT Policy

This policy applies to people, referred as 'users' using ICT resources provided by the University, including but not limited to;

- students enrolled at various constitute units of the University
- staff (teaching and non-teaching) employed by the University
- temporary, casual or agency staff working for or on behalf of the University
- contractors, consultants and suppliers working for or on behalf of the University
- visitors to the University

5: The ICT Resources Covered by the Policy

This policy applies to ICT resources and systems made available to the users by or on behalf of the University including but not limited to;

- personal computers, laptops and terminals
- peripherals such as printers, copiers, scanners and multimedia devices
- mobile devices such as smart phones and tablets
- networks with wired, wireless, dialup and/or internet connections
- internet services such as world-wide-web, blogs and wikis
- e-mail and other messaging, social networking or collaboration services such as blogs, chats and forums
- system and application software, services and databases
- removable media such as CDs, DVDs and USB drives

6: Guiding Principles for ICT Application

An ICT Application is an ICT resource (hardware, software, or a digital resource) provided to a user by the University. The University and its ICT Center, while providing an ICT Application or taking decisions regarding the ICT related activities will be guided by the following principles:

- Access: Provide unrestricted access to teaching, learning and research information to its stakeholders using ICT and also access to University services to stakeholders through ICT.
- Economy: Application ICT to improve economy in the practice of the University. The University will use ICT to reduce operation costs and improve teaching, learning and research quality.
- Efficiency and Effectiveness: Use ICT with a view to increase University's efficiency in delivery of services and improve effectiveness in achieving the expected results of the University.
- Relevance: Improve relevance of the learning experiences of the students at the University, and continuously use and adopt relevant ICT for the University.
- Transparency: Use ICT to foster openness in University system management and delivery of services to the stakeholders.
- Privacy: Use of ICT within the University to protect individual privacy as per the applicable law.
- Accountability: ICT application in the University shall improve accountability of the system for its operation.
- Sustainability: Reduce the costs of ICT related energy consumption as well as promote the sustainability of ICT solutions and sustainability through the application of ICT.
- Learner Centered: Provide ICT tools that empower the students and enable them to be responsible for their own learning.
- Pedagogy Driven: Develop ICT resources that would support subject and course specific pedagogical innovations and create new learning experiences in classroom practices.
- Quality Assurance: Integrate quality assurance strategies and their continuous development into ICT processes and services.

7: Areas of ICT Application

The following is a description of areas where ICT resources may be developed and made available to stakeholders for their efficient use.

7.1: Research:

Increasingly, research challenges are tackled by interdisciplinary teams, often distributed across institutions or countries and so the researchers are required to depend heavily on ICT to compute, analyse data and information, and prepare reports for the dissemination of research results. Use of ICT in research could take a variety of forms, including qualitative and quantitative data analysis, data visualization and reporting in refereed journals and social media. The University will endeavour to make its ICT resources available for creating conducive research environment. The University may undertake a range of activities to support research through the use of ICT, but not limited to the following:

- Provide data capture, analysis and management tools for both qualitative and quantitative data.
- Ensure the credibility of research through use of appropriate tools to check plagiarism.
- Organise training and capacity building activities to help researchers to use latest tools for research. Structure this effort as ICT Ecosystem for Research.
- To collaborate with local and regional partners to further develop research and e-Infrastructure capability.
- Strengthen the use of ICT by providing centralised and structured access to online databases, journals and resources over the Internet (e.g. MOOCs, INFLIBNET, NKN, NPTEL etc.).
- Provide improved administrative support systems to the researchers for efficient and effective management of research grants and other funding resources.
- Provide access to University's research publications and other products through a central repository
- Publish online editions of University journals for better reach and visibility
- Participate in regional, national and global discussions on collaborative research using ICT.

7.2: Admissions

The multi-campus and multi-disciplinary nature of the University necessitates the use of ICT to ensure effectiveness, efficiency and transparency of the admission process. The University may undertake a range of activities to support the admission process through use of ICT, but not limited to the following:

- Publication of admission related information over the Internet for better reach and visibility
- Provide online registration facility for prospective students
- Maintain a follow up and help prospective students through online support system and FAQs
- Conduction of online Entrance Tests for admission to
- University programmes

7.3: Human Resources

The increasing competitive environment and growing student volume poses a challenge to an academic institution. In this scenario, ICT can be used as a facilitator to increase effectiveness and efficiency of the services offered by the University and its constituent institutions. The University may undertake a range of activities to support human resources through the use of ICT, but not limited to the following:

- Support the non-teaching staff by standardising routine administrative activities, and automating their process flow
- Provide advance learning and up-gradation opportunities to the teaching staff through online training programmes and support
- Build an online community of teaching and non-teaching staff to provide horizontal communication channel
- Develop Knowledge Management Systems to capture and maintain the expertise for later use, particularly for curriculum development
- Document and share innovative practices through Knowledge
- Management System

7.4: Teaching and Learning

The use of ICT to provide support to the teaching and learning process has become an ingrained activity in educational institutions. A major benefit of ICT for the teachers is that they can make their classroom teaching more effective by making its judicious use. The students are also benefited due to possibilities for interaction beyond the classroom through ICT. ICT enabled teaching-learning encompasses a variety of techniques, tools, contents and resources aimed at improving the quality and efficiency of the teaching-learning process. Teachers in the higher education system today can use a variety of media and technologies inside and outside the classroom to make their teaching effective. ICT are used by teachers to catalyze the transformation of information into student learning. While using Internet related resources in the classroom, every care may be taken to address the appropriateness of the content and avoid inappropriate contents therein. The University may undertake a range of activities to support teaching and learning through use of ICT, but not limited to the following:

- Facilitate teachers to engage in selection and critical evaluation of digital content and resources (from Massive Open Online Courses - MOOCs, NPTEL etc.) to embed them teaching-learning process.
- Encourage teachers to contextualise open educational resources available on the Internet for the students of University.
- Encourage teachers to develop digital learning resources of their own. Facilitate teachers to collaborate and undertake projects to develop high quality digital learning materials for the students. The digital resources may include documents, presentations, animations, audio recordings and video clips. University needs to setup a media wing to professionally help teachers in this endeavour.
- Create appropriate online learning space through Learning Management System (LMS) to share the learning modules created by the teachers. Through LMS students will have authorised access to relevant modules.
- Provide recorded sessions across the campuses through podcasts (for audio sessions) and webcasts (for video sessions).

- Facilitate synchronous (e.g. chatting) and asynchronous (e.g. e-mail and forum) communication channels between teacher and student for off-campus academic discussion.
- Facilitate synchronous and asynchronous communication channels amongst students for peer learning.
- Provide real time sessions across the campuses through webinars and virtual classrooms.
- Allow online completion academic activities and submission of assignments, progress reports etc. in off-campus scenarios such as internships, fieldwork.
- Organize training on effective use of ICT for teaching and learning for every teacher. Such training may be organized within the University or faculty members may be deputed to attend external workshops.
- Provide training on effective use of ICT and social media in the University to the students.

7.5: Student Performance Evaluation

Student performance evaluation is the most critical aspect of University system as the gatekeeper of academic quality and credibility of the organization. Use of ICT has improved administration of tests in both online and offline scenario. The objective of the student evaluation system using ICT should include: providing an efficient mechanism to conduct examinations, improve transparency and credibility of the system, help declare the results error-free and in timely manner, and evaluate the students in a valid and reliable manner. The University may undertake a range of activities to support student evaluation through the use of ICT, but not limited to the following:

- Provide facilities for online registration for examinations, and share results online.
- Students should be informed about examination schedules and changes to schedules, if any, online.
- Create online systems for internal assessment and integrate the same with final student examination.
- Encourage teachers to use online testing system to be provided by the University for internal assessment.
- Provide feedback to students on their performance on a regular basis, on-line.
- Create question banks and share them through a repository.
- Use ICT for improving the credibility of the examination by putting practices in place to check impersonation and other malpractices.
- Use ICT to analyse evaluation data for preparing reports on student performance, evaluator performance etc.

7.6: Student Support

A support mechanism helps the students to excel and achieve their full potential. The traditional student support systems need to be supplemented with ICT to increase its scalability and availability. The University may undertake a range of activities to support students through use of ICT, but not limited to the following:

- Class-coordinators play an important role in student support system. An online communication and information distribution channel between a class-coordinator and his/her students need to be provided.

- Online support is required to drive University's centralized training and placement activity. It should integrate placement related services at University level, while providing institute- level programme-specific services to students through the activities such as Placement training, Placement related activities and management of students' portfolios.
- Continuous strategic contacts can be maintained with alumni through the use of ICT. An exhaustive alumni database needs to be prepared and made available to all the constituent institutions for use.
- Use ICT to provide various supplementary skills to students including soft skills, personality development. A blended learning approach can be adopted to facilitate online learning of such skills.
- Facilitate the data mining on learning analytics for student support.
- Use ICT to provide required information regarding hostel accommodation and to handle related complaints and feedbacks.
- ICT can be used to encourage students to actively participate in extracurricular activities. Individual student participations in these events can be recorded and made a part of their individual portfolios.

7.7: Community Engagement

ICT facilities can be used by the University to enhance its engagement with the society through extension activities. It may undertake a range of activities to support its extension activities through use of ICT, but not limited to the following:

- NSS and sports activities can to be supported with dedicated
- ICT systems to increase students' participation in them.
- University can use social media platforms to create awareness about health and other societal issues.
- University can create educational modules on societal issues (e.g. environment science) for general public and host them as open learning resources.

7.8: Administration

Apart from research and teaching, a major application of ICT can be in administration of the University. It will endeavour to connect all its Constituent Institutions to the University network and provide the services in a phased manner. It will develop a strategic plan to provide access to its key resources to all its students and teachers. The University may undertake a range of activities to support administration through use of ICT, but not limited to the following:

- Store the documents in digital form and provide authorised access to them
- Provide a communication channel between University and its constituent institutions for information exchange
- Standardise and automate the activities involved in academic administration for class and course management
- Standardise and automate the administrative processes of the University and its constituent institutions through an integrated system. The stakeholders should be able to access the required information through personalised dashboards
- Automate the generation of various compliance reports
- Provide need based automation support to University's staff to perform specific tasks
- Promote the use of office computing to support general office tasks

7.9: Quality Assurance

The transparency brought by ICT encourages quality assurance in an organization. The University will certainly and with definite focus work towards the quality assurance (encouraged by the use of ICT) in administration, teaching- learning and evaluation. The University may undertake a range of activities to support quality assurance through the use of ICT, but not limited to the following:

- ICT will help to improve the quality of administration and bring in transparency in the related processes through automated systems. They will also make the respective processes person-independent. The increased speed of operations will provide timely information.
- ICT will be used to facilitate data mining on learning analytics of students for programme improvements; to encourage cooperation amongst teachers; to standardise study material across the campuses through learning modules and LMS; and like.
- The University will enhance transparency in evaluation processes and the quality of evaluation through the use of ICT for collaboratively preparing question banks, developing automatic question paper generation systems, conducting online examinations wherever feasible, and for providing timely feedback to students etc.
- The quality assurance initiatives need to be supported by apt mechanisms for online feedback from various stakeholders and its analysis using ICT.
- Databases of teachers and domain-experts will be maintained and made available to constituent institutions as per their teaching, evaluation and research requirements.

8: ICT Infrastructure and System Maintenance

The valuable ICT assets must be managed to ensure their integrity, security and availability for valid educational and administrative purposes. While the university seeks to promote academic freedom and free exchange of ideas, some guidelines for the use of ICT are required. The guidelines are as follows.

8.1: University's Responsibilities

- ICT systems and infrastructure will be managed by the University's ICT Center.
- University will create adequate budgetary provision for maintenance of the ICT infrastructure and to implement this Policy.
- It will adequately ensure and provide for appropriate security, antivirus and password management systems.
- While the University will take all the necessary care to maintain its systems and servers, it accepts no responsibility for any loss or damage, consequential or otherwise, or loss of data arising from the use of its ICT Resources or due to the maintenance of its ICT Resources.
- Wherever possible, the University will use Open Source applications for providing services and reduce the total cost of running the ICT infrastructure.

8.2: Unacceptable uses of ICT resources by Users

Unacceptable use of the university's ICT resources may include but are not limited to the following.

- Attempt to access computers for which the concerned individual is not authorized
- Unauthorized access to another user's files
- Attempting to circumvent Network Access Control, including by-passing proxies and firewalls
- Monitoring or interception of network traffic without permission
- Probing for the security weaknesses of systems by methods such as port scanning, password cracking, without permission
- Unauthorized extension or retransmission of network traffic including the installation of unauthorized wireless access points, routers or switches
- Unauthorized reselling of University's ICT Systems and Services
- Unauthorized modification of university's data
- Unauthorized download, installation or running of programs or utilities that may flood the network, causing denial of service to other users
- Sharing of network access credentials with third parties for the purposes of defeating network authentication.
- Using the network to break into other networks
- Creation, retention, downloading or transmission of any offensive, obscene or indecent images or data, or any data capable of being resolved into obscene or indecent images or material
- Creation, retention or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety
- Infringement of Intellectual property rights including copyright, trademark, patent, design and moral rights
- Sending electronic mail that purports to come from an individual other than the person actually sending the message using, for example, a forged address
- Using the resources for unsolicited advertising or transmission of electronic mail with intent to defraud, often referred to as "spamming"
- Deliberate unauthorized access to networked resources, local or remote
- Deliberate activities that may result in either wasting of support staff time in support of systems or corrupting or destroying other users data violating the privacy of other users
- Denying services to other users
- Actions or inactions which intentionally, or unintentionally, aid the distribution of computer viruses or other malicious software
- Download, installation and use of unlicensed software on the
- University network and computers
- Any activity which comes within the purview of cyber laws of the land.

9: Information Security

The purpose of these guidelines is to identify and disseminate the framework and principles that guide institutional actions and operations in generating and sharing data and information.

Bharati Vidyapeeth (Deemed to be University), Pune (India)

9.1: Use of physical infrastructure

Security refers to the measures that shall be taken to ensure that physical availability of all ICT equipment is not compromised in any way. ICT equipment at the University falls under two categories (a) The College/Institute/ Department/Section/ Faculty/ Staff or "unit's" equipment and (b) the backbone equipment. Physical security of the former is the responsibility of the respective unit while the latter is the responsibility of the ICT Center. The following guidelines will be adhered to by all concerned.

- All the constituent units and offices shall be required to define an 'owner' of each piece (e.g. a computer, laptop, printer in an office) or group (say in a computer lab or server room) of equipment and that individual shall take the responsibility of ensuring its security
- All backbone equipment (except that housed within units) shall be the responsibility of ICT Center
- All the students and staff shall be required to identify themselves (either physically or electronically) for access to any common University computing facilities
- Only authorized staff will be permitted to open computer or related systems
- Students and other staff shall not tamper with any components of computer systems for whatever reason beyond what is required to carry out the basic user services
- No computer equipment and related accessories shall be carried out of the computer labs without explicit permission from an authority
- The heads of the constituent units and sectional heads in the University shall maintain ICT asset registers in order to monitor and track the assets.

9.2: Responsibilities of Users

The electronic data of the university either reside on University's central servers or on desktops, laptops and other mobile devices belonging to individual users. In either case, users must be aware of policy issues governing their protection and access. The following policy statements thus apply.

- All University data should be stored on centrally maintained corporate networked disc storage. In the event that such data is stored on user desktops, laptops and other mobile devices, it is the responsibility of the user to ensure its security, confidentiality and integrity with regular backup, password protection etc.
- All access to data stored in the central databases must be through standard interfaces provided for by the various information systems. Any attempt to gain access through any other means other than those sanctioned by the university constitutes security breach.
- Requests for access to all administrative data and the central systems in general need to be authorised by the relevant Data Owner after recommendation by the head of constituent institution or the section head.
- In the event that confidential information is protected by technical security mechanisms (physical or electronic) using passwords etc. and these mechanisms fail or are absent, users themselves are obliged to protect confidential information from public access.

9.3: Responsibilities of Technical Staff

The responsibility for protecting all corporate data stored in University's central systems (servers, database, network storage etc.) is the responsibility of the ICT Center. The guiding policies for this role are as stipulated below.

- All University data residing on the central network storage must be kept backed up on a regular basis. Frequency of backup needs to be determined by the frequency with which the data changes and the effort required to recreate the information if lost.
- Backup must be tested periodically to ensure that they support full system recovery. All restore procedures must be properly documented and tested on a regular basis, at least annually. Backup media must be stored in an off-site location and retrievable within 24 hours, 365 days a year.
- Data owners in their role as custodians of University data are responsible for defining and documenting the length of time during which data must be retained. ICT Center is responsible for ensuring that these requirements are adhered to.

9.4: Information Security related Policies

All involved stakeholders must follow applicable information security related policies as per involved contexts:

- Responsible Usage Policy for ICT Resources
- Online Content Management Policy
- Data Backup Policy

(Note: These policies are included in the Appendix.)

10: Online Content Publishing

University has worked hard to attain the high level of excellence in education, research, and outreach experiences. To maintain and build upon that reputation, it must concern itself with the image it projects. The web content publishing guidelines facilitate usability and consistency. Each constituent institution, unit, department, forum, and office, while having its own agenda, as a part of the whole, needs to be clearly identified with the University brand.

10.1: Avoid Redundancy

Constituent institutions should not repeat static information maintained elsewhere by the University. Instead their websites should provide link to that specific University information. Redundant information, especially different published versions, often causes confusion among the audience and there may be severe consequences if incorrect information is posted.

10.2: Ensure Content Validity

- The University controlled sites must be registered according to the guidelines
- Individual units at the University are responsible for the content on all of their Web pages
- Content must be continuously updated. It will follow all sections of this policy, as well as national laws and codes
- No official unit may go outside the University Web structure and represent itself on another Web server or domain without written approval from the University

- Visible credits such as "Site powered by..." or "Site created by..." are prohibited.

10.3: Copyright
- All web pages should follow copyright laws.
- Publishers of content must obtain permission from copyright holders to use text, photos, graphics, sounds, or movies to which the University does not hold copyrights.

11: Capacity Building for ICT Use

The University will take care of the following measures for the development of Human Resource in ICT:

- For the ICT Center staff to perform effectively and efficiently, they shall be continuously trained to enhance their skills so that they can meet the changing needs of the users. The ICT Centre shall put in place training and development plans to address the skill competencies of the staff
- Appoint at least one member of staff from each constituent institution as ICT Coordinator. ICT Coordinators will act as links between ICT Center of the University and respective constituent institutions
- Provide technical training, on efficient use of ICT services, to all teaching and non-teaching staff from all constituent institutions
- Provide training to the faculty on content development and to develop e-learning modules
- Provide functional training to all teaching and non-teaching staff to improve their ICT competency.
- Train researchers on University's ICT Ecosystem for Research to enable them to use ICT in their research process
- Train all the faculty members in the use of ICT for administration and for teaching and learning purposes.
- Train at least one staff members from each of the constituent institutions in software, hardware and network maintenance

12: Quality Assurance of ICT Resources and Services

In order to enhance and maintain the quality of ICT and ICT services, the ICT Center shall perform the following activities:

12.1: Quality Norms for ICT Services

- Continuously monitor the quality of ICT infrastructure and ICT services.
- Try to resolve 80% of all the technical problems within eight working hours after a complaint is received.
- Conduct at least 3 training sessions in a year to equip the end- users with relevant and practical ICT skills to facilitate effective and efficient use of ICT resources by them.
- Cost-effectively develop 70% application systems within three(3) to six(6) months of receiving requests.
- Ensure that 80% of digital network services (LANs/WANs) operate 24x7 in all departments of the university.
- Formulate and operationalize ICT policies within a reasonable time after their approval.
- Organize workshops, at least two in every six(6) months, on latest trends and practices in ICT.
- Establish an on-line help desk.

12.2: Disaster Recovery (DR) Plan

The University shall establish a disaster recovery planning capability which will develop and maintain coordinated plans, procedures and technical measures that would enable essential systems to be recovered following a disaster and provide assurance that these plans, procedures and measures are effective. A framework for disaster recovery may consider the following.

- Standards: The University shall develop standards for DR Planning based on generally accepted good practices.
- Continual improvement: The University shall establish a DR team to implement continual improvement of the DR planning capacity, the DR Plans and Standards. The DR Plans shall be peer-reviewed every two years and to follow any significant change to the architecture. The DR Plans shall be regularly audited for its compliance with the Standards.
- Disaster Preparedness: Recovery capabilities and plans shall be tested every two years in accordance with the Standards. The University shall identify capability and capacity measures designed to mitigate the consequences of a disaster. The University shall acquire and maintain resources necessary to ensure viability of the DR procedures.
- Reporting and Review: Compliance of the DR Plans with the Standards shall be reported through the Director, ICT Center. The Director, ICT Center shall ensure that this Policy is regularly reviewed.

12.3: Information System Audit

The University will conduct Information System Audit, at least once in two years, to ensure that the hardware, software, networks, ICT management, services etc., are all according to standards.

13: Management of ICT Policy

The domain of ICT is an evolving one. Considering the frequency of technology updation and obsolescence, the University will review and update its ICT Policy every three years. For this the University will have a formal setup as follows:

- The ICT Center will be headed by a senior technical professional. The support staff of the ICT Center will have expertise in ICT related fields such as network administration, data center administration, web site design, LMS management etc.
- Each constituent institution will have ICT Infrastructure Coordinator, e-Learning Coordinator and Website Coordinator to liaison with the ICT Center.
- The University will constitute an ICT Advisory Council under the chairmanship of the Vice-Chancellor, and some heads of constituent institutions and ICT experts from the field as members.
- A document describing the available ICT services and their possible use, will be circulated periodically to all concerned centres.

14: Appendix (Information Security related Policies)

- Responsible Usage Policy for ICT Resources
- Online Content Management Policy
- Data Backup Policy

Bharati Vidyapeeth (Deemed to be University), Pune (India)

14.1: Responsible Usage Policy for ICT Resources

Need for Responsible Usage Policy for ICT Resources
- Every entity of the University (e.g. University Departments, Institutes etc.) provides ICT resources (e.g. PC, Internet, Printer, Scanner etc.) to its staff.
- Responsible usage of these resources is mandatory to avoid undesirable consequences such as unlawful-usage, cyber-crimes, cyber-attacks etc.

This policy provides guidelines to avoid such scenarios.

Involved Terms
- **ICT Resources:**
  o Hardware Resources: Computing Devices (PC, Laptop, Mobile Phone etc.), Peripheral Devices (Printer, Scanner etc.)
  o Software Resources: System software (e.g. Windows), Application Software (e.g. MS-Office)
  o Service Resources: Internet, Institutional e-Mail Account
- **Custodian:** Any personnel to whom a respective ICT Resource is assigned

Guidelines for Entities of the University (e.g. University Departments, Institutes etc.)
- Entity must maintain a detailed account of ICT Resources owned and whom they have been assigned (their respective custodians)
- Entity must maintain a list of software required to perform its day-to-day activities (e.g. operating system, anti-virus, task-specific application software etc.)
- The entity must use only licensed software. In case of unavailability of licensed software, their open-source alternatives (e.g. OpenOffice) should be used.
- As per the legal software list, only job specific software must be installed on individual personnel's computers.
- Anti-virus software must be installed on every computer, and it should be updated on periodic basis (preferably on daily basis). In case of unavailability of licensed anti-virus software, free anti-virus software alternatives should be used (e.g. AVAST).
- Internet usage should be protected through a Firewall and individual login accounts, and its access reports should be monitored on periodic basis.

Guidelines for Personnel (staff of the entities)
- Any personnel is the custodian of assigned ICT Resource, and is responsible for its legal use. Personnel must use assigned ICT Resources only for official use.
- Personnel should access the Internet only for official use.
- Personnel should use only official e-mail account for official communications.
- Personnel must follow following generic guidelines on daily basis:
  - Use normal user account for daily activities (don't use Administrator account)
  - Properly shut-down a computer (don't just turn-off power switch)
  - Update anti-virus software on daily basis and perform full anti-virus scan on periodic basis (at-least once in a week)
  - Create hierarchical folder-subfolder-file structure to store your data (do not use C drive to store data)
  - Optimally use assigned peripheral devices (e.g. use printer in low-resolution, back-to-back and multi-page mode), and securely manage file-and-printer-sharing
  - Setup a backup routine for critical data on assigned ICT Resources
  - Take precautions (such as anti-virus scan) while using portable storage drives (i.e. pen drives)

*****

14.2: Online Content Management Policy

Any online content related activity must be backed by authorized communication.
Any online content must be edited or deleted as per predetermined schedule.

Need for Online Content Management Policy
- Entities of the University (e.g. University Departments, Institutes etc.) need to maintain repository of current as well as past information as per the guidelines from various regulatory authorities (e.g. NAAC, UGC, MCI etc.) on their websites.
- It is observed that entities of the University upload content on various online platforms (e.g. websites, social media pages, digital marketing sites, blogs etc.) but fail to keep its track. This leads to information chaos due to duplicate / wrong / irrelevant information.

Involved Terms
- **Online Content:** Digital content available on an online platforms (e.g. websites, social media pages, digital marketing sites, blogs etc.)
- **Content Management:** Upload/Edit/Remove/Monitor activities with online content
- **Content Owner:** Head of the entity whose information is uploaded on online platform (e.g. Heads of University Departments, Heads of Institutions etc.)
- **Platform Technician:** Personnel responsible to manage an online platform (e.g. website management personnel, social media management personnel etc.)

Guidelines to Manage Online Content
- Content is prepared and validated by the Content Owner.
- Content is communicated to respective Platform Technician through official communication whose trail must be maintained by all involved stakeholders.
- Content will be uploaded on online platform by respective Platform Technician.
- Edit/Remove activities related to uploaded content should be performed by Platform Technician only on receipt of an official communication from the Content Owner.
- Content Owner must verify any Upload/Edit/Remove activities performed by Platform Technician.

Guidelines to Monitor Online Content
- Content Owner must ensure availability of current and past content as per the guidelines from regulatory authorities (e.g. NAAC, UGC, MCI etc.), and periodically verify the same.
- Content Owner must maintain a register of online content owned by the entity along with respective timelines (e.g. platform-name, document-name, date-of-upload, date-of-edit, date-of-removal etc.)
- Content Owner must decide the criticality of online content and accordingly its monitoring frequency (e.g. once in a day, once in a week), and also its status (should be made available / should be removed)
- Content Owner must periodically monitor (at-least once in a week) all related online content, corresponding to involved entity (e.g. University Departments, Institutions etc.), with respect to maintained register.

Content Owner is responsible for any online content and not Platform Technician!

14.3: Data Backup Policy

It's not about whether a hard-disk will crash … it's about when it will crash!

Need for Data backup Policy
- Entities of the University (e.g. University Departments, Institutes etc.) need to maintain repository of current as well as past information as per the guidelines from various regulatory authorities (e.g. NAAC, UGC, MCI etc.), as well as to support its operations over the period.
- It is observed that corresponding data about an entity is generally scattered around multiple PCs used by different personnel (e.g. Clerks, Accountant, Administrative Officer, HODs, HOI etc.)
- Failure of storage on a PC leads to corresponding data loss, resulting in serious consequences proportional to criticality of lost data.
- Therefore all entities must have clarity about criticality, ownership and availability of data on perpetual basis.

This policy provides guidelines to avoid such scenario.

Requirements
- Two external hard-disks (labelled as *Backup-1* and *Backup-2*)
- A dedicated personnel entrusted with backup activity

Custodians
- Any personnel entrusted with a PC is the custodian of that PC. That personnel is responsible to maintain availability of critical information stored on that PC.
- Head of the entity (e.g. Heads of University Departments, Heads of Institutions etc.) is the custodian of both external hard-disks used for backup activity.

Backup Levels
1. Primary Backup: On the same PC (backup frequency - daily)
2. Secondary Backup: On *Backup-1* external hard-disk (backup frequency – weekly)
3. Tertiary Backup: On *Backup-2* external hard-disk (backup frequency – six monthly)

NOTE: Stated backup-frequencies are suggestions, and should be adjusted as per criticality of concerned information.

Activities to be performed by every personnel having a PC
- One-Time Activity:
  1. Create a dedicated partition and name it as *Backup-<Personnel Initials>* (e.g. Backup-SAK). If not possible to create a partition, then create a dedicated folder and name it as *Backup-<Personnel Initials>*.
  2. Identify all critical information (e.g. Word documents, Excel sheets, images etc.) stored on that PC.
  3. Copy that information to *Backup* location in a structured way using appropriate folder and sub-folder hierarchy.
- Daily Activity (to be performed every evening)
  1. Copy any important document worked upon during the day to *Backup* location (at appropriate folder hierarchy) at the end of every day.

Activities to be performed by Backup Personnel

- One-Time Activity:
    1. Take an external hard-disk and label it as *Backup-1*.
    2. Create a folder hierarchy as *Year-Month-Week* (e.g. 2021-July-Week3) in *Backup-1* hard-disk.
    3. Take another external hard-disk and label it as *Backup-2*.
    4. Keep both the hard-disks in the custody of Head of the entity.
- Weekly Activity (to be performed on every Saturday)
    1. Take the *Backup-1* hard-disk from the custody of Head of the entity.
    2. Copy respective *Backup* partitions/folders from all personnel's' PCs at appropriate *Year-Month-Week hierarchy*.
       NOTE: Check the contents using an anti-virus software before copying.
    3. Check the entire *Backup-1* hard-disk using an anti-virus software.
    4. Return *Backup-1* hard-disk in the custody of Head of the entity.
- Six-Monthly Activity (to be performed in June and December)
    1. Take *Backup-1* and *Backup-2* hard-disks from the custody of Head of the entity.
    2. Check both the hard-disks using an anti-virus software.
    3. Copy the contents of *Backup-1* hard-disk to *Backup-2* hard-disk in a folder named accordingly (e.g. 2021-JulyDecember).
    4. Verify the contents of both hard-disks for possible restoration purpose.
    5. Return *Backup-1* and *Backup-2* hard-disks in the custody of Head of the entity.
- Ad-hoc Activities (to be performed as and when required)
    1. Copy recent respective folder from *Backup-*1 hard-disk to a personnel's PC in case of any data loss scenario (e.g. hard-disk crash, unintentional deletion etc.) with custodians' consent.

*****

Bharati Vidyapeeth (Deemed to be University), Pune (India)