|| अंतरी पेटवू ज्ञानज्योत ||

KBCNMU

JALGAON

'A' Grade
NAAC Re-accredited
(3rd Cycle)

IT Operation and Maintenance Policy

Kavayitri Bahinabai Chaudhari
North Maharashtra University, Jalgaon

IT Operations and Maintenance Policy

1. Policy Statement:

1.1 Kavayitri Bahinabai Chaudhari North Maharashtra University, Jalgaon ("KBCNMU" or the "Institution") is highly dependent on technology to perform its activities on a daily basis. As a result, the Institution has adopted a formal approach to operating and maintaining its Information Technology ("IT") systems and resources.

2. Background:

2.1 Dedicated resources are required to support IT systems in production and ensure effective operations and troubleshooting when necessary. These include:

2.1.1 Sufficient system capacity (processing power, network access and bandwidth, data storage, etc.).

2.1.2 Monitoring procedures to proactively detect system issues or disruptions.

2.1.3 Procedures to answer users' service requests, as well as system problems, incidents or disruptions, in a timely manner.

2.1.4 Contracts with third party IT service organization(s) where it makes economic sense and allows for efficiencies to address the Institution's needs, compared to using internal resources.

2.1.5 Fully trained IT staff.

3. Policy Objective:

3.1 The objective of this policy is to define the roles, responsibilities and critical elements for the efficient operations and support of IT systems at the Institution.

4. Scope:

4.1 This policy applies to:

4.1.1 All Institution offices, schools, campuses and learning centres, including specifically all the stakeholders of the university.

4.1.2 All IT systems or applications managed by the Institution that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

5. Definitions:

5.1 "IT Problems" are conditions or situations (known or unknown) that can result in an incident.

5.2 "IT Incidents" are unplanned events which cause an interruption to, or a reduction in, the quality of the IT operations or services.

5.3 "Security Vulnerabilities" are IT problems that present specific risks to cyber security. Vulnerabilities that have a high probability of being exploited and that will highly impact the Institution (risk of operation disruption, data breach, etc.) are often labeled as "Critical" or "High".

6. Guiding Principles – Help Desk and User Support:

6.1 The UGC Computer Center, School of Computer Sciences as well as Computer Center (Examination) will act as the central point of contact for all IT technical requests.

6.2 UGC Computer Center, School of Computer Sciences ("IT Help Desk") will deal with the IT technical request from the academic schools, whereas Computer Center (Examination) ("IT Help Desk") will deal with the IT technical request from the administrative sections.

6.3 All the stake holders should report in written the IT technical request in the format (See format section) for hardware maintenance to the corresponding IT Help Desk.

6.4 Upon receipt of the written request the IT Help Desk will use the following guidelines to prioritize its response to requests:

Urgent	Criteria	Response Time (*)
Urgent	Requests for issues having a significant and immediate impact on the Institution's operations. For example: • An issue affecting all or a large number of users. • An issue preventing users to access critical applications or data or impacting critical functions (e.g. access to network shares, email, or academic courses). • An information security incident or vulnerability with a critical/high severity/risk. • An issue affecting the ability of a class to be delivered or a meeting to take place. • Other as directed (removal of access rights for an unscheduled terminated user for example).	Within 2 hours
High	Requests for issues having an important impact on the Institution's operations. For example: • An application error affecting a small group of users. • An issue impacting important functions in a system. • An information security incident or vulnerabilities with a medium/high severity/risk. • Other as directed.	Within 4 hours
Normal	Requests for issues having a limited or non-immediate impact on the Institution's operations. For example: • An issue affecting one person only. • An issue impacting a non-critical function in a system (reporting for example). • A security incident or vulnerability with a low/medium severity/risk. • A question on how to use a non-critical functionality.	Within two working days

Low	Issues that have no material or immediate impact on the Institution's operations. For example: • A "cosmetic" request, to improve a system functionality "look and feel" or a minor non-functional change to a system.	Within a week if possible.

(*) The response time corresponds to the time to process the request, including analyzing and classifying the request, attributing a request to the IT staff, and dispatching of the IT staff. This time does not indicate when the ticket must be resolved.

6.5 The assigned IT Staff will respond to all requests submitted to the IT Help Desk within a one- week period where possible. If a request cannot be processed within a one-week timeframe, the IT Staff should inform the user who submitted the request.

6.6 If the IT staff from IT Help desk is unable to resolve the IT technical request, a report regarding the same will be submitted to the concerned to take help from external agencies in resolving the issue/replacing the H/W part.

7. Guiding Principles – IT Problem and Incident Management:

7.1 Where possible, the Institution will take preventative measures to prevent problems from occurring and minimize the impact of incidents that do occur by addressing identified problems as quickly as possible. Examples of preventative measures include the implementation of high- availability and redundant systems and back-up solutions.

7.2 Problems and incidents with a priority of urgent or high must be reported within two hours of detection to contain the issue, and if possible, prevent any further impact.

7.3 KBCNMU will conduct investigations into problems and incidents with priorities of urgent or high to determine the root cause of the issues, to remediate the issues and return to a normal situation in a timely manner.

7.4 The following key performance indicators and metrics will be used by KBCNMU to monitor IT problems and incidents:

7.4.1 Number of total problems and incidents by severity (and category where applicable).

7.4.2 Number of problems and incidents resolved.

7.4.3 Number of problems and incidents unresolved, with the time since opened and description of why they are still open.

7.4.4 Average time to resolve problems and incidents.

8. Guiding Principles – IT Asset Management:

8.1 The use of non-standard equipment, applications or technology services must be approved by the IT director.

8.2 A list of IT assets shall be maintained by all the schools and administrative sections in accordance with the Fixed Assets Policy. The following equipment should be included in the list:

8.2.1 Computer and network hardware (desktops, servers)

8.2.2 Mobile computing devices (smartphones, tablets, laptops)

8.2.3 Computing storage media (tapes and backups)

8.2.4 Software (applications, software sources and licenses)

8.3 All computer hardware (as defined above) must be brought to the notice of IT Help desk for identification and traceability.

8.4 All stakeholders must protect IT assets against the threats of: unauthorized access, theft, loss, or destruction.

8.5 Mobile computing devices (as defined above) must never be left unattended without physical security protection in place, such as: security cable attached to the equipment, locked in a secure cabinet, in a locked office, storage area, or vault.

8.6 The list of IT assets should be updated by concerned school/administrative section whenever an asset's status, location or ownership is changed.

8.7 Before disposing or recycling IT assets, the concerned school/administrative section will ensure all sensitive information is securely and safely removed from the device.

9. Guiding Principles – Systems Replacement:

9.1 For IT systems that will no longer be supported by a vendor (including operating systems and application versions), the Institution will upgrade or replace the system at least one year prior to the end of the vendor's support, where possible.

9.2 KBCNMU will replace IT systems and / or equipment that no longer provide an acceptable level of performance as follows:

9.2.1 Servers should be upgraded depending upon the performance of the server and considering the need to replace the server after 5 years, after due recommendation from the technical committee nominated by Hon'ble Vice Chancellor or equivalent.

9.2.2 Desktops and laptops can be replaced approximately after 5 years, if required after due recommendation from the technical committee/person nominated by Hon'ble Vice Chancellor or equivalent.

9.2.3 O/S should be upgraded to the latest version every 3 years, where ever possible.

9.2.4 Smartphones should be replaced approximately after 5 years, if required after due recommendation from the technical committee/person nominated by Hon'ble Vice Chancellor or equivalent.

10. Guiding Principles – IT Infrastructure and Network:

10.1. The Institution will ensure its IT infrastructure availability and performance is continuously monitored (i.e. 24 hours a day, all working days a week).

10.2. Follow section 7 of this policy to react to any network infrastructure availability or performance issue.

10.3. The configuration of systems backups and the recovery processes will follow the IT Continuity, Backup and Recovery Policy.

10.4. The IT Department will be involved in defining the IT technical requirements (i.e. IT and security) for new NMU projects, including new technology, new or renovated buildings, etc.

10.5. Planned maintenance will occur during the scheduled maintenance window.

11. Guiding Principles – Vulnerability and Patch Management:

11.1 The following activities will be carried out to assist KBCNMU in the identification of vulnerabilities to systems and applications:

11.1.1 Scanning of web applications that are publicly accessible at a minimum every year.

11.1.2 Scanning of web applications that are not publicly accessible at a minimum every two years.

11.1.3 Network vulnerability scanning at a minimum every year.

11.1.4 Penetration testing, including a detailed review of the system security configuration, at a minimum every five years.

12. Guiding Principles – Applications Management:

12.1 Only authorized software and licensed products must be used and installed by all stake holders.

12.2 The request for development of new applications must have approval from Hon'ble Vice Chancellor or equivalent.

12.3 The purchase of software or commercial off the shelf ("COTS") applications must follow the Purchasing Policy of the university.

12.4 Planned maintenance will occur during the scheduled maintenance window.

13. Annual Rate Contract:

13.1 KBCNMU will have an annual rate contract for procurement/maintenance of IT Assets like (pen drive, CD/DVD, Toners/Cartridges, Networking components etc.)

14. Exceptions to the Policy

14.1 Exceptions to the guiding principles in this policy must be documented and formally approved by the IT Director.

14.2 Policy exceptions must describe:

14.2.1 The nature of the exception

14.2.2 A reasonable explanation for why the policy exception is required

14.2.3 Any risks created by the policy exception

14.2.4 Evidence of approval by the IT Director

15. Inquiries:

15.1 Inquiries regarding this policy can be directed to the IT Director.

Online Examination Centre (OEC)

To promote online examinations culture, university has setup Online Examination Centre (OEC) having state of the art infrastructural facilities with adequate technical manpower for conducting various skill-based courses for students, training programs for teachers, administrative staff, real time examinations, mock tests for recruitment as well as competitive examinations and a facility centre for students of the university. The set-up includes 04 High End rack servers with firewall security and 231 nodes distributed in 06 spacious laboratories, connected with structured network; having committed internet connectivity under the aegis of RUSA, Maharashtra.

The centre was formally inaugurated by His Excellency, Chancellor of the University Shri. CH. Vidyasagar Rao, Governor of Maharashtra on 20th December 2017.

Aims and Objectives:

1. Facility for conduct of preparatory tests for competitive examinations as well as examinations conducted for employment eligibility and fellowships etc.
2. To conduct online tests for recruitment of students by government and non-government organizations.
3. Recruitment activities carried out by Central Training & Placement Cell (CTPC) using online tests for pre-recruitment in various industries.
4. Provide facility to give hands-on training to students to enrich ICT based skills.
5. To facilitate resources for conduct of skill based/value added certificate courses.
6. To extend ICT facility for capacity building of teaching and administrative staff.
7. Facility centre for various day to day online requirements of various stake holders of the university.
8. Online Common Entrance Test for admission to UG/PG/Ph.D. programmes.

Utilization Policy:

To avail the facilities at OEC, it is mandatory to seek approval of Hon'ble Vice Chancellor. After approval, concern School/Department/Institute, need to fill-up prescribed proforma along with approval, endorsed with Director of the School/Head of the Department or Administrative officer and submit it to Co-ordinator, along with specific remarks for network setup required for the event, license software installation etc.

Maintenance Procedure:

The OEC is following policy issued by Computer Centre of the university under which a complaint is registered in prescribed format to the Head, Computer Centre.

KAVAYITRI BAHINABAI CHAUDHARI
NORTH MAHARASHTRA UNIVERSITY, JALGAON

Application format for maintenance of Computer Hardware

NORTH MAHARASHTRA UNIVERSITY, JALGAON.	
Machine Make/Model : (HP/HCL/ACER/IBM)	Date:
Location No.:	
Name of Department :	
Concern person:	
Nature of Problem:	
Sign.of concern person:	
For AMC office use only	**Complent No. :**
Remark :	
	OK / INCOMPLETE
Call attended by :	
Date:	
Time:	Sign.of concern person:

Vice Chancellor
Kavayitri Bahinabai Chaudhari
North Maharashtra University, Jalgaon

For approval purpose

- History of Document: Issued with approval of Vice Chancellor.

Approved by	Date	Resolution No.
(i) Academic Council	04/12/2020	AC A-79/2020
(ii) Management Council		

****