



U.P. Pandit Deen Dayal Upadhyaya Pashu Chikitsa Vigyan Vishwavidyalaya
Evam Go-Anusandhan Sansthan (DUVASU), Mathura

उ.प्र. पंडित दीन दयाल उपाध्याय पशुचिकित्सा विज्ञान विश्वविद्यालय एवं गो-अनुसंधान संस्थान (दुवासु), मथुरा



IT Policies & Guidelines

2022



कुल सचिव

उ० प्र० पं० दीनदयाल उपाध्याय
पशु चिकित्सा विज्ञान वि० एवं गो अनुसंधान संस्थान
मथुरा

Table of Contents

Sr. No.	Chapter	Page Number
1	Need for IT Policy	3
2	IT Hardware Installation Policy	5
3	Software Installation & Licensing Policy	7
4	Network (Intranet & Internet) Use Policy	8
5	Email Account Use Policy	10
6	University Database (of eGovernance) Use Policy	11
7	Hostels Wi-Fi Use Policy	13
8	Responsibilities of Computer Center/AKMU	13
9	Responsibilities of Department	15
10	Responsibilities of the Administrative Department	17
11	Guidelines for Those Running Application or Information Servers	17
12	Guidelines for Desktop Users	18
13	Video Surveillance Policy	18
14	Web Application Filter	19
	Appendices	
1	Campus Network Services	20
2	Requisition Form for E-Mail Account	22
3	Application for Net Access ID Activation	23
4	Requisition for CCTV Footage	24

1. Need for IT Policy

- The purpose of the University's information technology policy is to safeguard, maintain, and guarantee that the campus's information technology infrastructure is used judiciously and appropriately.
- This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets that the University accesses, creates, manages, and/or controls.
- The policy addresses information assets such as data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

Intranet and Internet services have undoubtedly become the most important resources in educational institutions and research organizations. Recognizing the significance of these services, U.P. Veterinary University took the initiative and established basic network infrastructure in the university's academic complex. Over the last ten years, not only have active users of network facilities increased many folds, but so have web-based applications. This is a welcome change in the academic environment of the university.

Agricultural Knowledge Management Unit (AKMU) (ARIS Cell) is the department that has been given the responsibility of running the University's intranet & Internet services. The Cell provides internet connectivity to different Departments of Colleges and Offices of the University as well as hostel through LAN and wireless access point. This is useful for the retrieval of information and data from various sources on various aspect needed by students and teachers. This facility not only helps students, scientists and teachers of the University but also the farmers and animals –owners as their problems are addressed by making use of the latest information in that field. AKMU is running the Firewall security, DHCP, DNS, email, web and application servers and managing the network of the university. U.P. Veterinary University is getting its Internet bandwidth from RailTel. Total bandwidth availability from RailTel source is upto 100 Mbps.

The widespread use of the Internet has influenced network performance in three ways:

- Internet traffic over the Wide Area Network (WAN) is a potential bottleneck when compared to the speed of the Local Area Network (LAN).
- When users have unrestricted Internet access, non-critical downloads may clog the traffic, resulting in poor Quality of Service (QoS) and affecting critical users and applications.
- When computer systems are networked, viruses that enter the LAN via Intranet quickly spread to all other computers on the network, exploiting operating system vulnerabilities.

Too many concurrent users on high-speed LANs attempting to access Internet resources via a limited bandwidth strain the available Internet bandwidth. Every download increases Internet traffic. This raises costs and, eventually, lowers the Quality of Service and Quality of Experience. The solution is to reduce Internet traffic. Computer viruses attach themselves to files, spread quickly when files are shared, and are difficult to remove. Some can corrupt the files and reformat the hard drive, causing significant financial loss to the organization. Others simply attach to files and replicate themselves, consuming network space and slowing the network.

Apart from that, a significant amount of employee time is lost while a workstation is scanned and cleaned of the virus. The majority of virus attacks on networks are caused by emails, unsafe downloads, file sharing, and web browsing. Viruses attach themselves to files, replicate quickly, and cause untold damage to network data.

They have the potential to slow down or even bring the network to a halt. It is difficult to contain a virus once it has spread throughout the network. Many man-hours and possibly data are lost in restoring network security. So preventing it as soon as possible is critical. As a result, in order to secure the network, AKMU has taken appropriate measures such as installing firewalls, access control, and virus checking and content filtering software at the gateway. However, in the absence of clearly defined IT policies, convincing users of the steps taken to manage the network is extremely difficult. Users often believe that such restrictions are unwarranted, unjustified, and infringe on their freedom.

IT security measures will be ineffective and may not align with management objectives and desires if strong management policies are not in place. Furthermore, because of the dynamic nature of information technology, information securities in general, and thus policies that govern the information security process, are also dynamic. They must be reviewed on a regular basis and modified to reflect changing technology, changing IT user community requirements, and operating procedures.

It should be noted that University IT Policy applies to technology administered centrally by the University or by individual departments, information services provided by the University administration or by individual departments, individuals of the University community, or authorized resident or non-resident visitors on their own hardware connected to the University network. This IT policy also applies to resources managed by central administrative departments, such as the Library, AKMU, Laboratories, University Offices, or hostels and guest houses, or residences where the University provides network access.

Furthermore, all faculties, students, staff, departments, authorized visitors/visiting faculty, and others who may be granted access to the University's information technology infrastructure must abide by the guidelines. Certain violations of the University's IT policy by any university member may even result in disciplinary action by the University authorities. If there is evidence of illegal activity, law enforcement agencies may be called in.

Applies to

Stake holders on campus or off campus

- Students: Diploma, UG, PG, Research
- Employees (Permanent/ Temporary/ Contractual)
- Faculty
- Administrative Staff (Non-Technical / Technical)
- Higher Authorities and Officers
- Guests

Resources

- Network
- Devices wired/ wireless
- Internet Access
- Official Websites, web applications
- Official Email services
- Data Storage
- Mobile/ Desktop /Laptops/ server computing facility
- Documentation facility (Printers/Scanners)
- Multimedia Contents

2. IT Hardware Installation Policy

University network users must take certain precautions when having their computers or peripherals installed so that they are not inconvenienced by service interruptions caused by hardware failures.

a) Primary User

The "primary" user is the person in whose cabin the computer is installed and is primarily used by him/her. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make a plan and assign someone to be in charge of compliance.

b) End User Computer Systems

Apart from the client PCs used by users, the university will consider servers that are not directly administered by AKMU (ARIS Cell) to be end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems that are acting as servers and providing services to other users on the Intranet/Internet, even if registered with the AKMU (ARIS Cell), are still considered "end user" computers under this policy.

a result, it is critical to bring all computers into compliance as soon as it is discovered that they are not.

j) Computer Center/AKMU Interface

When the Computer Center/AKMU discovers a non-compliant computer affecting the network, it will notify the individual in charge of the system and request that it be brought into compliance. This notification will be sent via email or phone. The individual user will follow up on the notification to ensure that his or her computer achieves the required compliance. The AKMU will assist the individual in achieving compliance as needed.

3. Software Installation & Licensing Policy

Individual departments/cells should ensure that any computer systems purchased have all licensed software (operating system, antivirus software, and necessary application software) installed. In accordance with the country's anti-piracy laws, University IT policy prohibits the installation of pirated/unauthorized software on university-owned computers and computers connected to the university campus network. In such cases, the university will hold the department/individual personally liable for any pirated software installed on computers in their department/individuals' cabins.

a) Operating System and its Updating

Individual users should ensure that their computer systems' operating systems are up to date in terms of service packs/patches via the Internet. This is especially important for all Microsoft Windows-based computers (both PCs and Servers). Users updating their operating systems help their computers fix bugs and vulnerabilities in the operating system that are periodically detected by Microsoft and for which it provides patches/service packs.

b) Antivirus Software and its updating

Anti-virus software should be installed and active on all computer systems used by the university. The primary user of a computer system is responsible for maintaining compliance with this virus protection policy. Individual users should ensure that their computers have up-to-date virus protection software installed and maintained.

He or she should ensure that the software is functioning properly. It should be noted that any antivirus software running on a computer that is not updated or renewed after the warranty period is practically useless. If these responsibilities appear to be beyond the end user's technical abilities, the end user is responsible for contacting AKMU for assistance.

c) Backups of Data

Individual users should backup their crucial data on a regular basis. Virus infections frequently destroy data on a computer. Recovery of deleted files may be impossible without proper backups. Preferably, the computer's hard disc should be partitioned into multiple volumes, such as C, D, and so on, during the OS installation process.

The operating system and other software should be on the C drive, with user data files on the other drives (e.g. D, E). In most cases, only the C volume is corrupted when there is a virus problem. In this case, formatting only one volume will prevent data loss. It is not, however, a foolproof solution. Aside from that, users should keep their important data on CDs/DVDs or other storage devices such as pen drives, external hard drives.

d) Noncompliance

U.P. Veterinary University faculty, staff, and students who do not follow this computer security policy put themselves and others at risk of virus infections, which can result in damaged or lost files, inoperable computers, and lost productivity. There is also a risk of infection spreading to others and confidential data being revealed to unauthorized persons. An individual's non-compliant computer can have serious consequences for other people, groups, departments, or even the entire university. As a result, it is critical to bring all computers into compliance as soon as it is discovered that they are not.

e) Computer Center/AKMU Interface

When the AKMU discovers a non-compliant computer, it will notify the individual in charge of the system and request that it be brought into compliance. This notification will be sent via email or phone. The individual user will follow up on the notification to ensure that his or her computer achieves the required compliance. The AKMU will assist the individual in achieving compliance as needed.

4. Network (Intranet & Internet) Use Policy

The University IT Policy governs network connectivity provided via WiFi or an authenticated network access connection. Except for local applications, the Network must be continuously maintained and supported by the AKMU. Network issues with the University should be reported to the AKMU.

a) IP Address Allocation

The AKMU should assign an IP address to any computer (PC/Server) that will be linked to the university network. Each building's / V LAN's assigned IP address range should be followed by departments in a methodical manner. Therefore, only IP addresses from that Address pool will be assigned to any computer connected to the network from that building. Additionally, each network port in the space where that computer will be connected will have internal binding with that IP address set up to ensure that no one else uses it uninvitedly from any other location.

When a new computer is installed in any location, the user must obtain an IP address from the AKMU / respective department. An IP address assigned to a specific computer system should never be used on another computer, even if that other computer belongs to the same person and is connected to the same port. IP addresses are assigned to computers but not to ports.

b) DHCP and Proxy Configuration by Individual Departments /Cells/ Users

The use of any computer at the end user location as a DHCP server to connect to more computers via an individual switch/hub and distribute IP addresses (public or private) should be strictly avoided, as it is considered an absolute violation of the university's IP address allocation policy. Similarly, configuring proxy servers should be avoided because it may interfere with AKMU's service. Noncompliance with the IP address allocation policy will result in the computer's connection to the network being disconnected. After receiving written assurance of compliance from the concerned department/user, the connection will be restored.

c) Running Network Services on the Servers

Individual departments/individuals connecting to the university network via LAN may run server software, e.g., HTTP/Web server, SMTP server, FTP server, only after informing the AKMU in writing and meeting the university IT policy requirements for running such services. Noncompliance with this policy is a direct violation of the university's IT policy, and their connection to the network will be terminated. The AKMU accepts no responsibility for the content of machines connected to the Network, whether they are University or personal property. Where potentially harmful software is discovered, the AKMU will be forced to disconnect client machines. A client machine may also be disconnected if its activity has a negative impact on the Network's performance.

Access to remote networks via a University network connection must adhere to all network policies and rules. This applies to all networks to which the University Network is linked. At AKMU, network traffic will be monitored for security and performance reasons. Impersonating an authorized user while connecting to the Network is a violation of this agreement and will result in the connection being terminated.

d) Dial-up/Broadband Connections

Computer systems on the University's campus-wide network, whether university or personal property, should not be used for dial-up/broadband connections, as this violates organization security by bypassing firewalls and other network monitoring servers. Noncompliance with this policy may result in the computer system's IP address being withdrawn.

e) Wireless Local Area Networks

This policy applies to all wireless local area networks, whether departmental or hostel-based. Departments or hostels must register each wireless access point with AKMU, including Point of Contact information, in addition to the requirements of this policy. Wireless local area networks with unrestricted access are not permitted in departments or hostels. Authentication or MAC/IP address restrictions must be used to restrict network access. Data and passwords must be encrypted. If a department wishes to have an inter-building wireless network, it must first obtain permission from the university authorities, whose application may be routed through the In Charge, AKMU.

5. Email Account Use Policy

It is advised to use the University's e-mail services for formal University communication as well as for academic and other official purposes in order to increase the efficiency of disseminating important information to all faculties, staff, students, and the University's administrators. Delivery of messages and documents to the campus and wider communities, or to specific user groups and individuals, will be made easier with email for official communications. Official University communications are messages sent by the University to its staff, faculty, and students. These messages may contain administrative information like details about human resources, policy messages, and messages for the entire University, official announcements, etc. The e-mail address must be kept active by continued use in order to receive these notifications. Faculty and staff can access the email service by visiting <https://www.duvasumathura.com:2096/> and entering their User ID and password. Users can contact AKMU for an email account and the default password for the university by submitting an application in the required format. Users should be aware that by using the email service, they agree to the following policies:

- The facility should be used primarily for academic and official purposes, with some personal use permitted.
- Using the facility for illegal/commercial purposes is a direct violation of the University's IT policy and may result in the facility being withdrawn. Unlicensed and illegal copying or distribution of software, as well as the sending of unsolicited bulk e-mail messages, are examples of illegal use. Furthermore, the transmission of threatening, harassing, abusive, obscene, or fraudulent messages/images.
- The user should not open any email or attachment from an unknown or suspicious source. Even if it is from a known source, and if it contains any attachment that appears suspicious or suspicious, the user should obtain confirmation from the sender about its authenticity before opening it. This is critical for the user's computer's security, as such messages may contain viruses that have the potential to damage the valuable information on your computer.
- The user should not share his/her email account with others because the individual account holder is personally liable if the email account is misused.
- While using computers shared by other users, any email account that was accidentally left open by another user should be closed immediately without peering into its contents. While using computers shared by other users, any email account that was accidentally left open by another user should be promptly closed by the user who has occupied that computer for its use, without looking into its contents.
- Impersonating another person's email account is a serious offence under the University's IT security policy.

- It is ultimately the responsibility of each individual to keep their e-mail account free of violations of the University's email usage policy.

The policies outlined above are broadly applicable even to email services provided by third-party providers such as Hotmail.com, Yahoo.com, and others, as long as they are used from the university's campus network or by using the resources provided by the university to the individual for official use even from outside.

6. University Database (of e Governance) Use Policy

This Policy applies to the databases managed by the university administration as part of eGovernance. Data is an essential University resource for providing useful information. Even if the data is not confidential, its use must be safeguarded. U.P. Veterinary University has its own policies for database creation and information access, as well as a more general policy for data access. These policies, when combined, outline the university's approach to both access and use of this university resource.

A. Database Ownership:

U.P. Veterinary University is the data owner for all institutional data generated at the university.

B. Custodians of Data:

Individual sections or departments generate data that is part of the University's database. They may have custodial responsibilities for some of that data.

C. Data Administrators:

The data Custodian may delegate the outlined data administration activities to some of the officers in that department.

D. MIS Components:

The university's Management Information System requirements can be broadly classified into seven categories for the purposes of eGovernance. These are:

- MANPOWER INFORMATION MANAGEMENT SYSTEM (MIMS)
- STUDENTS INFORMATION MANAGEMENT SYSTEM (SIMS)
- FINANCIAL INFORMATION MANAGEMENT SYSTEM (FIMS)
- PHYSICAL RESOURCES INFORMATION MANAGEMENT SYSTEM (PRIMS)
- PROJECT INFORMATION MONITORING SYSTEM (PIMS)
- LIBRARY INFORMATION MANAGEMENT SYSTEM (LIMS)
- DOCUMENT MANAGEMENT AND INFORMATION RETRIEVAL SYSTEM (DMIRS)

Here are some general policy guidelines and parameters for data users in Sections, Departments, and Administrative Units:

1. The University's data policies prohibit the distribution of data that can be traced back to an individual outside the university.
2. Data from the University's Database, including data collected by departments or individual faculty and staff, is intended solely for internal university use.
3. The data resources required to carry out one's official responsibilities/rights are defined by one's role and function. The university makes information and data available based on those responsibilities/rights through its data access policies.
4. Data directly identifying a person and his/her personal information may not be distributed to outside persons or agencies in any form, including all government agencies, surveys, and other data requests. All such requests must be directed to the University Registrar's Office.
5. Requests for information from courts, attorneys, etc. are handled by the University's Registrar Office, and departments should never respond to requests, even if they are served with a subpoena. All requests from law enforcement agencies must be directed to the Office of the University Registrar for processing.
6. No information, including 'Directory Information,' may be released to any outside entity for commercial, marketing, solicitation, or other purposes. This includes organizations and businesses acting as agents for the university or its departments.
7. The Registrar, Controller of Examinations, and Finance Officer of the University will prepare/compile and submit all reports for the UGC, MHRD, and other government agencies.
8. Database users who repackage data for others in their unit must notify the recipients of the data access issues mentioned above.
9. Tampering with the database by the department or an individual user is against IT policy. Tampering includes, but is not limited to:
 - Modifying/deleting data items or software components through the use of unauthorized access methods.
 - Changing or deleting data items or software components on purpose, even by authorized individuals or departments.
 - Causing a database, hardware, or system software crash, thereby destroying the entire or a portion of the database with ulterior motives by any individual.
 - Trying to breach database server security.

Such data tampering actions by university members or outside members will result in disciplinary action by the university authorities against the offender. If there is evidence of illegal activity, law enforcement agencies may be called in.

7. Hostels Wi-Fi Use Policy

- The use of wireless infrastructure in hostels is to improve access to the internet for academic purposes and to browse U.P. Veterinary University's exclusive online resources (licensed online journals) for students, faculty, and staff.
- The availability of the signal will vary from location to location, as will the signal strength. It is not required that every area on every floor of every block have the same signal strength, coverage, and throughput.
- Wireless internet access is only available on a limited basis, and neither students nor residents of the hostels can request it.
- The availability of wireless services is solely at the discretion of U.P. Veterinary University, which reserves the right to stop/interrupt services at any time for any technical reason.
- The access points provided in hostels are U.P. Veterinary University property, and any damage or loss of the equipment will be considered a serious breach of U.P. Veterinary University's code of conduct, and disciplinary action will be initiated against the student/s found guilty of the loss or damage of the Wireless Infrastructure or the corresponding equipment in the hostels buildings. In the event of a loss or damage to the wireless infrastructure, U.P. Veterinary University will assess the damage and recover it from all students living on that floor/building/hostel.

8. Responsibilities of Computer Center/AKMU

a) Campus Network Backbone Operations

1. AKMU manages, maintains, and controls the campus network backbone and its active components.

2. AKMU operates the campus network backbone in such a way that service levels required by University Departments and hostels served by the campus network backbone are maintained within the constraints of operational best practices.

b) Maintenance of Computer Hardware & Peripherals

AKMU is in charge of maintaining university-owned computer systems and peripherals that are either under warranty or out of warranty.

c) Receiving Complaints

AKMU may receive complaints from users if any of the computer systems or peripherals that they maintain are malfunctioning. The designated person in AKMU receives complaints from users of these computer systems and works with service engineers from the respective brands of computer systems (which are under warranty) to resolve the problem within a reasonable time frame. Problems with out-of-warranty computer systems are resolved at the

computer centre. AKMU may receive complaints from departments/users; if they notice any network-related problems, such complaints should be made via email/phone. If a user is unable to access the network due to a network-related problem at the user's end, AKMU may receive a complaint. Such complaints are typically made over the phone. The designated person in AKMU receives user complaints and coordinates with network hardware user/service engineers or the internal technical team to resolve the problem within a reasonable time frame.

d) Scope of Service

AKMU will be responsible for resolving hardware-related issues, as well as OS and as well as network-related issues or network-related services.

e) Installation of Un-authorized Software

AKMU or its service engineers should not encourage users to install unauthorized software on their computer systems. They should strictly refuse to comply with such requests.

f) Physical Demarcation of Campus Buildings' Network

1. AKMU is responsible for the physical connectivity of campus buildings that are already connected to the campus network backbone.
2. AKMU is responsible for the physical demarcation of newly constructed buildings from the "backbone." It essentially means that the AKMU will decide where the fiber optic-based backbone terminates in the buildings. The manner in which the building is to be connected to the campus network backbone (whether via fiber optic, wireless, or any other media) is also under the control of AKMU.
3. AKMU will consult with the client(s) to ensure that end-user requirements are met while the integrity of the campus network backbone is maintained.
4. While it is not the University's policy to actively monitor Internet activity on the network, such activity may be examined when a problem occurs or when optimizing traffic on the University's Internet links.

g) Network Expansion

AKMU is also in charge of major network expansion. AKMU reviews existing networking facilities and the need for possible expansion as and when required.

h) Wireless Local Area Networks

1. Where access via Fiber Optic/UTP cables is not possible, AKMU considers providing network connectivity via wireless connectivity.

2. The AKMU is authorized to consider Departments' or Divisions' applications for radio spectrum from AKMU prior to the implementation of wireless local area networks.

3. AKMU has the authority to limit network access to Cells, departments, or hostels via wireless local area networks through authentication or MAC/IP address restrictions.

i) Electronic logs

Electronic logs generated as a result of network traffic monitoring should only be kept until the administrative need for them has passed, at which point they should be destroyed.

j) Global Naming & IP Addressing

AKMU is responsible for providing a consistent forum for campus network service allocation, such as IP addressing and domain name services. The AKMU monitors the network to ensure that these services are used correctly.

k) Providing Net Access IDs and email Accounts

AKMU issues Net Access IDs and email accounts to individual users in order for them to use the campus-wide network and email services provided by the University after receiving requests on the prescribed proforma.

l) Disconnect Authorization

AKMU reserves the right to disconnect any Department, cell, or hostel from the campus network backbone if its traffic violates the practices outlined in this policy or any network-related policy. In the event that a Department, or cell, hostel machine, or network severely degrades the normal flow of traffic, AKMU makes every effort to resolve the issue in a way that has the least negative impact on the other members of that network. If a Department or Division is disconnected, AKMU specifies the conditions that must be met in order for the Department or Division to be reconnected.

9. Responsibilities of Department

a) User Profile Any Centre, department, cell, or other entity may connect to the University network using a legitimate user account (Net Access / Captive Portal ID) to verify affiliation with the university. AKMU will provide a user account upon completion of the prescribed application form and submission to AKMU. Once a user account is assigned for accessing the university's computer systems, network, mail and web services, and other technological facilities, the account holder is personally liable and accountable to the university for all actions taken with that user account. As a result, users are advised to take reasonable precautions such as using complex passwords, not sharing passwords with others, not writing down passwords in a place where others can see them, changing passwords frequently, and keeping separate passwords for Net Access Id and email account ID to prevent unauthorized use of their user account by others.

It is the user's responsibility to understand the university's IT policy and to follow the guidelines in order to make proper use of the university's technology and information resources.

b) Information supplied by departments or cells for publication on/updating the U.P. Veterinary University website. All Departments or Cells should provide updated information about themselves on a regular basis (at least once in a month or earlier). To be sent to the AKMU in hardcopy or softcopy. This policy applies to advertisements/tender notices published in newspapers as well as events organized by Departments or Cells. After receiving written requests, the AKMU can provide links to any web pages that must be created for any specific purpose or event for any individual department or faculty. If such web pages are to be directly added to the university's official web site, the relevant department or individual must provide the necessary content pages (and images, if any) in a format that is exactly compatible with the existing web design/format. Furthermore, such requests should be forwarded to the In Charge, AKMU, along with a soft copy of the contents, well in advance.

c) Security by connecting to the network backbone, the department agrees to follow the University IT Security Policy and this Network Usage Policy. Coordination with a Point of Contact (POC) in the originating department is used to resolve any network security incidents. If a POC is not available to contact, the security incident is resolved by disconnecting the offending computer from the network until the user/POC meets the compliance requirements.

d) Network Equipment and Accessories Preservation Routers, switches, fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries are the property of the university and are maintained by the AKMU and respective departments. Tampering with these items by the department or an individual user is against IT policy.

e) Enhancements to the Existing Network Any addition to the existing network made by a department or an individual user must strictly adhere to the university network policy and must be approved by the appropriate authority and reported to the AKMU. For any network expansions, the following procedures must be followed according to University Network policy:

1. All internal network cabling should be CAT 6 UTP as of today.
2. UTP cabling must adhere to structured cabling standards. To connect to the network, no dangling UTP cables are used.
3. UTP cables must be properly terminated on both ends in accordance with structured cabling standards.
4. Managed switches should be used only. This type of management module should be web-enabled. Managed switches allow for web-based management, allowing AKMU to monitor the health of these switches from anywhere. However, the department/individual member will be solely responsible for the hardware maintenance of such an extended network segment.

5. Because managed switches require IP address allocation, this can be requested from AKMU.

f) Campus Network Services Use Agreement

All university members seeking network access via the university campus network backbone should read the "Campus Network Services Use Agreement." This is available on the university's website. This policy's provisions are deemed to be a part of the Agreement. Any department or individual who uses the campus network is deemed to have accepted the university's IT policy. It is the responsibility of the user to be aware of the University's IT policy. Ignorance of the existence of university IT policy does not excuse any user's violations.

g) Enforcement AKMU scans the University network on a regular basis for violations of the Network Use Policy. Failure to comply may result in the individual responsible for the violation of IT policy and guidelines losing service.

10. Responsibilities of the Administrative Department

The AKMU requires the most recent information from the various Administrative Departments in order to provide network and other IT facilities to new organization members and withdraw these facilities from those leaving the university, as well as to keep the U.P. Veterinary University web site content up to date. The following types of information may be required:

- Information on New Appointments
- Information on Service Termination
- New Enrollment Information
- Expiry of Studentship/Removal of Names from Rolls Information
- Important Events/Achievements Information
- Detailed information on various rules, procedures, and facilities.

11. Guidelines for Those Running Application or Information Servers

An application or information server may be run by a department. They are responsible for the upkeep of their own servers.

- 1) Obtain an IP address for the server from AKMU.
- 2) Retrieve the server's hostname from the DNS server for IP address resolution.
- 3) Make certain that only the services required to run the server for the intended purpose are enabled on the server.
- 4) Ensure that the server is adequately protected against virus attacks and intrusions by installing the necessary software, such as anti-virus, intrusion prevention, personal firewall, anti-spam, and so on.

5) The operating system and other security software should be updated on a regular basis.

12. Guidelines for Desktop Users

These guidelines are meant for all members of the U.P. Veterinary University Network User. Due to the increase in hacker activity on campus, University IT Policy has put together recommendations to strengthen desktop security. The following recommendations include:

1) All desktop computers should have the most recent version of antivirus software. Also, the setting that schedules regular updates of virus definitions from the central server should be retained.

2) When installing a desktop computer, all operating system updates and patches should be installed. Furthermore, operating system updates and patches should be applied on a regular and ongoing basis. The frequency will be determined by balancing productivity loss (while patches are applied) with the need for security. Each machine should be cycled once a week. Security policies should be set at the server level and applied to desktop machines whenever possible.

3) The password should be hard to guess.

4) The guest account must be deactivated.

5) In addition to the suggestions above, AKMU suggests a regular backup strategy. It should be noted that even with all of the above procedures, the possibility of a virus infection or hacker compromise exists. Backing up data on a regular basis (daily and/or weekly) will mitigate the impact of a machine failure.

13. Video Surveillance Policy

The system consists of the following components: fixed position cameras; monitors; digital video recorders; storage; and public information signs. Cameras will be placed strategically around campus, primarily at the entrance and exit points of sites and buildings. No camera will be hidden from view, and none will be able to focus on the front or back yards of private residences. Signs will be prominently placed at strategic points on campus, as well as at the campus's entrance and exit points, to inform staff, students, visitors, and members of the public that a CCTV Camera installation is in use. Although every effort has been made to ensure the system's maximum effectiveness, it is not possible to guarantee that the system will detect every incident occurring within the area of monitoring.

Purpose of the system

The system was installed by the University with the primary goal of reducing the threat of crime in general, protecting the university's premises, and assisting in ensuring the safety of all staff, students, and visitors while respecting individuals' privacy. These objectives will be met by monitoring the system to:

- Prevent those with criminal intent
- Assist in crime prevention and detection
- Facilitate the identification, apprehending, and prosecution of criminal and public order offenders
- Facilitate the identification of any activities or events that may warrant disciplinary proceedings against staff or students, and assist in providing evidence to managers and/or a member of staff or student against whom disciplinary or other action is being taken, or is threatened to be taken. It is understood that University members and others may have concerns or complaints about the system's operation. Any complaint should be directed to the AKMU as soon as possible. CCTV footage was provided by the University (AKMU) in response to requests from individuals using the prescribed proforma.

14. Web Application Filter

Application	Management	Staff	Students	Guest
Captive portal Session	2 concurrent sessions / user			
Sites Blocked	Porn, torrents, Proxy & Hacking, Gambling, Marijuana, Criminal Activity			
YouTube	Allow	Allow	Time based	Allow
YouTube Educational	Mandatory Certificate needs to be purchased			
What's App	Allow	Allow	Time based	Allow
Facebook	Allow	Allow	Time based	Allow
Skype or Video calling	Allow	Allow	Time based	Allow
Entertainment	Allow	Time based	Time based	Allow
TV news Channel	Allow	Allow	Time based	Allow
Online Game	Deny	Deny	Deny	Deny
Windows Update	Allow	Allow	Allow	Allow

Default Block Category in Firewall

- Weapon
- Phishing and fraud
- Militancy and Extremist
- Gambling
- Pro-Suicide and self-Harm
- Criminal Activity
- Marijuana
- Intellectual Piracy
- Hunting and Fishing
- Legal highs
- Controlled substances
- Anonymizers
- Sexually Explicit
- Nudity

Appendix I

Campus Network Services

Use Agreement Before applying for a user account/email account, please read the following important policies. By signing the application form for a Net Access ID (user account)/email account, you agree to follow U.P. Veterinary University's IT policies and guidelines. If you do not follow these policies, your account/IP address may be terminated. It is only a summary of the university's key IT policies. The detailed document can be obtained by the user from the website and various intranet servers. A Net Access ID is a username and password combination that allows you to access University computer systems, services, campus networks, and the internet.

a) Accounts and Passwords

The user of a Net Access ID agrees not to share the Net Access ID with anyone else. Furthermore, the Net Access ID will only be used for educational/official purposes. The User ensures that the Net Access ID will always be password protected. The User will not reveal his or her password or Net Access ID to anyone. Network IDs will be created only for students, staff, and faculty who are currently enrolled at the University. When students, staff, and faculty leave the University, their Net Access ID, email address, and associated files are deleted. No User will be permitted to have more than one Net Access ID at the same time, with the exception of faculty or heads who hold more than one portfolio and are entitled to a Net Access ID related to the functions of that portfolio.

b) Limitations on the use of resources

AKMU reserves the right, on behalf of the University, to close the Net Access ID of any user who is deemed to be using excessive amounts of storage space or whose actions otherwise limit the use of computing resources for other users.

c) Data Backup, Security, and Disclaimer

AKMU will not be liable for the loss or corruption of data on an individual user's computer as a result of the user's use and/or misuse of his/her computing resources (hardware or software), or for any damage that may result from the advice or actions of an AKMU staff member while assisting the user in resolving network/computer related problems. Despite AKMU's reasonable efforts to ensure data integrity, security, and privacy, the User accepts sole responsibility for backing up files in the assigned Net Access ID, storage space, or email Account. Furthermore, AKMU makes no guarantees about the security or privacy of a User's electronic messages. The User agrees to be held liable for improper use of equipment or software, including copyright violations, and agrees to defend, indemnify, and hold AKMU, as a subsidiary of U.P. Veterinary University, harmless from any such liability or expenses. U.P. Veterinary University reserves the right to change and update these policies at any time without prior notice to the User.

d) Account Termination and Appeal Process

Accounts on U.P. Veterinary University network systems may be terminated or disabled with little or no notice for any of the aforementioned reasons, as well as for other inappropriate use of computing and network resources. If the user believes that such termination is unjustified, or that there are mitigating circumstances for the user's actions, he or she may approach the In Charge, AKMU, justifying why this action is not justified.

Appendix II

**U.P. Veterinary University, Mathura
AKMU
Requisition Form for E-Mail Account**

1. Full Name : _____
(First Name) (Middle Name) (Last Name)

2. Employee Id : _____

3. Department : _____

4. Mobile No: _____

5. Email Mail Id : _____

Date:
.....

Signature of Applicant:

AKMU Use only.....

The following email ID is created for Prof. /Dr. /Mr. /Ms.

_____ on@

Signature on Behalf of In Charge,
AKMU, U.P. VETERINARY UNIVERSITY

Appendix III

**U.P. Veterinary University, Mathura
AKMU
Application for Net Access ID Activation**

2. Full Name : _____
(First Name) (Middle Name) (Last Name)

2. Employee Id/Student Enrollment No : _____

3. Department/College/Institute: _____

4. Mobile No: _____

5. Email Mail Id : _____

Date:
.....

Signature of Applicant:

AKMU Use only.....

Net access ID is activated for the applicant.

Signature on Behalf of In Charge,
AKMU, U.P. Veterinary University

Appendix IV

**U.P. Veterinary University, Mathura
AKMU
Requisition for CCTV Footage**

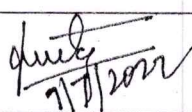
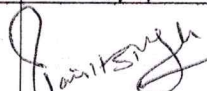
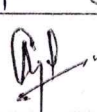
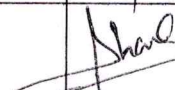
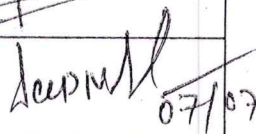
1. Name of Applicant : _____
 2. Employee / Student Id : _____
 3. Department : _____
 4. Mobile No: _____
 5. Email Mail Id : _____
 6. Date of Footage : _____ Time : From _____ To _____
 7. Camera Location : _____
 8. Description : _____
- Date: Signature of Applicant:

AKMU Use only.....

CCTV Footage is given to Applicant.

Signature on Behalf of In Charge,
AKMU, U.P. Veterinary University

IT Policies & Guidelines formulation Committee

S. No.	Name	Designation	Signature
1.	Dr. Sarvajeet Yadav Professor & Head	Chairman	 7/7/2024
2.	Dr. Pawanjeet Singh Assistant Professor	Member	
3.	Dr. Amit Singh Assistant Professor	Member	
4.	Dr. Shanker K. Singh Assistant Professor	Member	
5.	Dr. Deep Narayan Singh Assistant Professor	Member	 07/07/2024