Acceptable use of Information Assets Policy

Vishwakarma University

Title: Acceptable use of Information Assets	**Doc No.:**
Approval Date: 18-07-2020	**Review:** Annual
Effective Date: 19-07-2020	**Department:** System and Technology

Ver. No	Release Date	Owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

The purpose of this policy is to establish acceptable use of all information assets, electronic devices and network resources at VU in conjunction with its established information security policies & procedures, culture of ethical and lawful behavior, openness, trust, and integrity.

2. Scope

All Staff, contractors, consultants, temporary and other third party contractors at or outside the VU, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned by the VU, or to devices that connect to the VU's network or reside at a VU's site.

3. Objective

VU provides computer devices, networks, and all other assets to meet Objectives, Goals, and Initiatives and must manage the responsibly to maintain the confidentiality, integrity, and availability of its information assets. Objective is to make the Staff of information assets aware to comply with VU policies and protects the VU against damaging legal issues.

4. Policy Statement

4.1. General Requirements

- All Staff are responsible for exercising good judgment regarding appropriate use of VU's resources in accordance with VU's policies, standards, and guidelines. VU's resources shall not be used for any Personal, Unlawful or Prohibited purpose.

- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, and network traffic.
- Devices that affect other devices or Staff on the VU's network may be disconnected. Information Security department prohibits unauthorized audit scans on Internal & External network.

4.2. System Accounts

- Staff are responsible for the security of data, accounts, and systems under Staff's control.
- Password should not be shared with anyone, including other personnel, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
- Staff must maintain passwords in accordance with the Password Policy.
- Staff must ensure through legal or technical means that proprietary information remains within the control of VU at all times.
- Conducting VU's business that results in the storage of proprietary information on personal or non-VU controlled environments, including devices maintained by a third party with whom VU does not have a contractual agreement, is prohibited.

4.3. Computing Assets

- Staff are responsible for ensuring the protection of information assets that also includes the use of software and devices.
- Laptops left at VU must be properly secured or placed in a locked drawer or cabinet. Promptly report any theft of VU's assets to the incident response team.
- All PCs, laptops, and workstations must be secured with a password-protected screensaver with the automatic activation feature set to 5 minutes or less. Staff must lock the screen or log off when the device is unattended.
- Devices that connect to the VU's network must comply with the Bring your own device (BYOD) Policy.
- Do not interfere with corporate device management or security system software, including, but not limited to, antivirus, firewalls and servers.
- Staff should use the printer, data cards and scanner for official work only.
- All the pen drives that are assigned to Staff should be returned to System Administrator by end of the day. If the pen drive/data card is kept with the user after office hours, logs shall be maintained by System Administrator and authorized by information security officer.
- Data cards shall be assigned to user based on business requirement and need basis.

4.4. Network Use

Staff are responsible for the security and appropriate use of VU's network resources under Staff's control. Using VU's resources for the following is strictly prohibited:

- Causing a security breach to either VU's or other network resources, including, but not limited to, accessing data, servers, or accounts to which Staff are not authorized; avoiding user authentication on any device; or sniffing network traffic.
- Causing a disruption of service to either VU's or other network resources, including, but not limited to, ICMP floods, packet spoofing, denial of service, heap or buffer overflows, and forged routing information for malicious purposes.
- Introducing honeypots, honeynet, or similar technology on the VU's network without authorization.
- Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video, and software.
- Exporting or importing software, technical information, encryption software, or technology in violation of international or regional export control laws.
- Use of the Internet or VU's network that violates the Internet usage policy, or local laws.
- Intentionally introducing malicious code, including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and key loggers.
- Port scanning or security scanning on a production network unless authorized in advance by CISO.

Staff must report any weaknesses in VU's computer security to the appropriate authority. Weaknesses in computer security include unexpected software or system behavior, which may result in unintentional disclosure of information or exposure to security threats.

4.5. Electronic Communications

The following activities are strictly prohibited

- Inappropriate use of communication channels and equipment, including, but not limited to, supporting illegal activities, and procuring or transmitting material that violates VU's policies or the safeguarding of confidential or proprietary information.
- Sending Spam via e-mail, text messages, pages, instant messages, voice mail, or other forms of electronic communication.
- Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Use of a VU's e-mail or IP address to engage in conduct that violates VU's policies or guidelines. Posting to a public newsgroup, bulletin board, or blog with a VU's e-mail or IP address represents VU to the public; therefore, Staff must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the VU.

4.6. Disposal of Information Assets

- Staff should avoid creating multiple copies of confidential and sensitive information.
- Staff should take into consideration the sensitivity of information before disposing it off

5. Enforcement

Staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with VU.

6. Reference Document

- HR-IT policy
- Bring Your Own Device Policy
- Password Management policy

7. Distribution List

The following Staff have access to this policy:

- All Staff, contractors, consultants, temporary and other third party contractors of VU.

8. Acronyms/Definitions

- VU: Here it refers to Vishwakarma University
- Staff: Here it refers to Teaching Staff/ Non-Teaching Staff/ Office Staff/ Peons
- Honeypot, honeynet: Network decoys that serve to distract attackers from valuable machines on a network. The decoys provide an early warning for intrusion detection and detailed information on vulnerabilities.
- Spam: Electronic junk mail or junk newsgroup postings. Messages those are unsolicited, unwanted, and irrelevant.