INDIRA GANDHI NATIONAL TRIBAL UNIVERSITY, AMARKANTAK, MP, INDIA.

(A Central University established by an Act of parliament)

IT POLICY OF IGNTU – DECEMBER, 2018

(W.E.F.- 21 December, 2018)

VERSION I

Preamble

I. Definition of terms

II. Objectives

III. Scope

IV. Roles and Responsibilities

V. Policy Awareness

VI. Changes to the policy

VII. Enforcement

VIII. Policy on use of Computer

IX. Policy on use of Internet

X. Offences and Penalties (As per IT Act, 2000)

XI. Access Control Policy

XII. Data/ Information Security Policy

XIII. Network Policy

XIV. Physical Security

XV. Cyber Security and Safety Measures

Conclusion

Preamble:

In today's digital era, it is utmost importance to have a legal framework for effective use of computer infrastructure in the IGNTU (A Central University). The Information Technology (IT) Policy of the IGNTU University defines rules, regulations, and guidelines for proper utilization as well as the effective maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities along with users.

For the purpose of this policy has drafted to effective and efficient use of the term 'IT Assets includes (PC) or desktop devices, portable and mobile devices, networks including wireless networks, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

Misuse of these resources may lead to result in unwanted risk and liabilities for the IGNTU. It is, therefore, expected that these resources are used primarily for IGNTU related purposes and in a lawful act and ethical professional way.

I. Definition of terms:

- ✓ Computer Uses: The intention of University policies regarding computer as well as network infrastructure usage is to protect all individuals affiliated with determinant the University, including Teaching Faculty, Non-Teaching staff and students which are functionally dependent on Main Campus and remote sub-campus or RCM Centers which are affiliated to IGNTU.
- ✓ Inappropriate use exposes the University to risks, including virus attacks, compromise of network systems and services, and possible legal liability from intruders.

II. Objectives:

- ✓ An act to provide equal legal treatment for the transactions and business carried out by University users.
- ✓ IT Policy serves for matters connected therewith or incidental thereto on the University Cyberspace digital infrastructure as well as all dependent sub-campus of IGNTU.

III. Scope:

- ✓ To build a secure and resilient cyberspace for the teaching faculties, Non-Teaching staff's and students for progressive growth.

IV. Roles and Responsibilities:

It is mandatory that to appoint one dedicated or unit or Committee may establish and prepare blueprint of IGNTU network infrastructure.

Hence, the new (UNIC- 'University Network and Internet Center') center can develop at Campus which shall be used effectively and efficiently for monitor and procure new advanced infrastructure. Also, this center may help to provide service based on requests to address the issues of concerns users.

The Committee will be exploring to offer the best service towards the users as given below:

1. Conduct a risk audit of likely security and privacy risks at premises with help of third-party vendor or else invite security auditors to do assessment.
2. Discuss with Competent authority and Submit report with safety measures to strengthen the University cyberspace.

3. To evaluate and adjust the Information Security Program periodically with permission of Competent authorities. (The Vice Chancellor/ Registrar or a Nodal officer of University)
4. System Analyst and other technical staff members are required to implement the Cyber Security and safety measures.
5. Purchase required equipment's through prior permission as per seeking approval from authority to make safer cyberspace.
6. University Technical member shall appoint to as "Chief Cyber Security Officer" (CCSO's) to give legal opinion mining with consultation of learned experts. And give supporting hands in all above.
7. Cyber Forensic officer should attend the training from top Indian and oversees to adapt world's best contemporary practices at University campus.
8. Team or Committee shall do a visit of leading national institute or central University across the region of India which may explorer the best solution and adopt it in IGNTU University with prior permission of the competent authority.

9. To make a plan and do arrangements to invite an external Network security Auditor and finds the vendor party who can offer defense mechanisms to safeguard to the IGNTU internal intranet and internet infrastructure.

V. Policy Awareness:

Users who violate any acceptable use policy will be subject to disciplinary action, up to and including loss of privileges and/or expulsion, and may be at risk for civil or criminal prosecution as per IT Act 2000.

All violations will be handled in accordance with Indira Gandhi National Tribal University policies with respect to IT Act 2000.

Employee training and education programme:

- ✓ With the permission of competent authority of University, a training programme for all employees who have access to covered data and information should be arranged with an invited expertise across the India.
- ✓ It is mandatory to conduct awareness programme for newly joined Employees in University Campus as well as other dependant remote campus.

- ✓ In the interaction meet with newly admitted students give quick presentation to promote best practices of IT infrastructure and warn misuse lead to legal punishment as the IT act 2000.
- ✓ Use digital flex to promote best practices do's and don'ts ponder pints of cyber safety measures.

VI. Changes to the policy:

- ✓ In order to protect critical information and data, and to comply with looking into IT Act, 2000.
- ✓ To monitor and review will be continuous process to adopt and amends the existing policy time to time update and upgrade.
- ✓ As per contemporary times, with consent of legal advisory, special invitee expert's opinion and competent nodal authorities of the University sought to be done.
- ✓ It will be amendments of existing rules shall be bind to all users**.**

VII. Enforcement:

- ✓ This 'IT policy of IGNTU' will enforced in main campus of IGNTU and which are affiliated with IGNTU exclusively.

- ✓ The IT Policy of IGNTU will be enacted with effect from all latest version as per near completion of the compilation by time to tome or updated or upgraded version with number.
- ✓ As per competent authority approval it will be w.e.f. the same and applicable to all IGNTU employees.

VIII. Policy on use of Computer:

Desktops – Personal Computers (PCs) issued or provided to teaching and non-teaching staff in the course of carrying out their duties.

Laptops/Netbooks - Portable Personal Computers issued or provided to teaching and non-teaching staff in the course of carrying out their duties.

IX. Policy on use of Internet:

- All users shall register the client system and obtain one time approval from the competent authority before connecting the client system to the IGNTU network servers.
- Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security.

- The Internet will be used to promote ICT for educational purpose ultimately. The misuse may lead to fellow the violation of rules and regulation as per IT Act, 2000.
- To strengthen the ecosystem for creation as well as protection of Intellectual Property.
- To undertake policy, promotion and enabling actions for compliance to international security the best practices and conformity assessment (product, process, technology & people) and incentives for compliance.

X. Offences and Penalties: (As per IT Act, 2000)

Users may violate any acceptable use policy will be subject to disciplinary action, up to and including loss of privileges and/or expulsion, and may be at risk for civil or criminal prosecution as per IT Act 2000 or amended latest one.

XI. Access Control Policy:

Without permission mobile phones or any gadgets or electronic photography devices are not allowed in restricted or prohibited area or in confidential documents room.

XII. Data/ Information Security Policy:

Tempering of the official records:

User indulging in tempering official records of the University may be at risk or criminal prosecution or as per IT Act 2000.

Data security policy:

All Offices may take up backup drive manually on the external HDD on official hard disk. Also, it may keep in confidential cupboard with consents of redirecting officers or authorities.

XIII. Network Policy:

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures.

XIV. Physical Security:

To develop, adopt, evolve and notify standards for seamless interoperability of internal access of files.

XV. Cyber Security and Safety Measures:

Cyber security measures:

Indian Computer Emergency Response Team-means an agency established under sub-section (1) of Section 70 B [As per IT Act, 2000];

In case, if IGNTU University website would hack then Core administrator should inform to CERN-In with an approval of competent nodal authority of the University.

Conclusion:

The objective is to build capacity as well as enable teaching and non-teaching University department to create a cyber resilient IT set up for progressive growth.