HR Information Security Policy

Vishwakarma University

Ver. No	Release Date	Owner	Approved By	Change details

Restricted

Title: HR- Information Security Policy	**Doc No.:**
Approval Date: 15-01-2020	**Review:** Annual
Effective Date: 16-01-2020	**Department:** Human Resources/Establishment

1.0	16-01-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Overview

VU holds great amounts of **RESTRICTED** information. Information security is very important to help protect the interests and confidentiality of the VU and its

interested Parties. It cannot be achieved by technical means alone and must also be enforced and applied by people, and this policy addresses the same along with Human Resources being the primary objective.

2. Scope

The scope is to define the functioning of the VU focusing on the manpower & IT that is used to run the VU. This policy applies to all those personnel working in the VU as staff, contractors and also covers the aspect where any staff who requires access to VU's information systems or information of any type or format (paper or electronic).

3. Summary

This HR- Information Security Policy has been structured with the purpose to provide an overview of the VU's policies and to define the terms of employment with VU**.** The HR Dept. is supposed to brief all staff about all the VU's policies. Any questions about terms and procedures hereunder should be directed to the HR Department. It is the responsibility of every staff to understand and adhere to the terms laid down hereunder.

Owing to the nature of the VU's business, its growth and the amendments in law there is an ongoing need to revise policies and procedures of the VU. Therefore, VU retains the right to update this Policy to keep up with such changes as and when there is a need. To the extent that any policy or benefit is subject to interpretation, such interpretation will be determined by VU at its sole discretion within the confines of Indian laws.

In the event of alterations to policies and procedures like the addition of new policies, staff will be notified in writing by the HR Department. In the event of any future conflict or confusion with regard to any change of a policy, the most recent policy will take precedence.

The terms and conditions of a staff's appointment letter or any other format with context to staff and the VU, form a part of terms of these Policies and may be read in conjunction with the same.

4. Human Resource Security Policy

4.1. Prior to employment

4.1.1. Screening

As per ISMS HR Procedure, Screening of the Candidate shall be carried out.

Consultants/Contractors/staff recommended by the Vice Chancellor(s)/management screening procedure is waived off.

Information on all candidates being considered for positions within the VU is collected and handled in accordance with Indian legislation existing in the Pune jurisdiction. Depending on applicable legislation, the candidates are informed beforehand about the screening activities.

4.2. During Employment

All staff/contractors are to follow Clear Desk and Clear Screen Policy.

Management responsibilities shall include ensuring that staff and contractors:

a) Are properly briefed on their information security roles and responsibilities prior to being granted access to confidential information or information systems

b) Are provided with guidelines to state information security expectations of their role within the VU

c) Are motivated to fulfill the information security policies of the VU

d) Achieve a level of awareness on information security relevant to their roles and responsibilities within the VU

e) Conform to the terms and conditions of employment/association, which includes the VU's security policy and methods of working

f) Continue to have the appropriate skills and qualifications and are educated on a regular basis.

If staff and contractors are not made aware of their information security responsibilities, they can cause considerable damage to the VU. Motivated personnel are likely to be more reliable and cause fewer information security incidents.

4.3. Terms And Conditions Of Employment

The agreement with staff and contractors states their and the VU's responsibilities for the functioning within the VU and in relation to information security.

The agreements for staff or contractors reflect the VU's policies for the functioning of information security in addition to clarifying and stating:

a. That all staff and contractors who are given access to confidential information are also briefed upon the guidelines of information security.
b. Responsibilities for the clarification of information and management of VU's assets associated with information, information processing facilities and information services handled by the staff or contractor.
c. Responsibilities of the staff or contractor for the handling of information received from Interested parties;
d. Actions to be taken if the staff or contractor disregards the VU's security requirements.

Information security roles and responsibilities should be communicated to job candidates during the pre-employment process.

The VU ensures that staff and contractors agree to terms and conditions concerning information security, appropriate to the nature and extent of access they will have to the VU's assets associated with information systems and services.

Where appropriate, responsibilities controlled within the terms and conditions of employment should continue for a defined period after the end of the employment.

A Non- Disclosure Agreement (NDA) shall be signed by all staff, contractors.

4.4. Information Security Awareness And Training

All staff of the VU and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in VU policies and procedures, as relevant for their job function.

Awareness, education and training can be part of, or conducted in collaboration with, other training activities, for example general IT or general

security training. Awareness, education and training activities shall be suitable and relevant to the individual's roles, responsibilities and skills.

An assessment of the staff/contractors understanding is conducted at the end of an awareness, education and training course to test knowledge transfer.

4.5. Compliance With Rules And Regulations

By signing the Appointment letter an staff is deemed to have expressed his/her acceptance of all the policies, rules, regulations, terms and conditions framed from time to time by the concerned authorized officers.

During employment, the terms of employment of staff/ contractors shall be governed by the policies and rules framed from time to time covering, among others, Discipline, Code of Conduct etc.

4.6. Confidentiality And Non-Disclosure

Whether information in written or verbal, or contained in computer hardware or software, disk, hard disk, tape or other media, this information is of substantial value, highly confidential and is not known to the general public. Such Information is being provided and disclosed to the staff, contractor solely for use in connection with his/her employment or work of the VU. NDA is to be signed by all staff/ contractors. Signing to be followed as per Procedure.

4.7. Alteration In The Terms Of Employment

VU reserves the right to make reasonable changes to the duties of a staff, contractor according to the needs of the operation including, relocating/shifting such staff's workplace and / or transferring such staff to serve at any other location of the VU.

The VU reserves the right to make reasonable changes to any terms or conditions of employment of any staff with prior notice.

4.8. Termination And Change Of Employment

Information security responsibilities and duties that remains valid after termination or change of employment is defined, communicated to the staff or contractor and enforced.

Changes of responsibility or employment are managed as the termination of the current responsibility or employment combined with the initiation of the new responsibilities or employment.

The Human Resources function is generally responsible for the overall termination process and shall work together with the supervising manager of the person (Principal, Dean, HOD) leaving to manage the information security aspects of the procedures. In the case of a contractor provided through an external party, this termination process is undertaken by the external party in accordance with the contract between the VU and the external party.

HR Department shall inform staff, customer or contractors of changes to personnel and operating arrangements.

4.9. Disciplinary Action

There shall be a formal and communicated disciplinary process in place to take action against staff who have committed an information security breach.

Disciplinary action shall be taken by the management depending upon the severity of the event.

√ **Immediate Termination**

Under the circumstances of Sexual Harassment, Immediate Termination is valid and applicable or as may be prescribed under Applicable Law.

4.10. Discharge/Dismissal/Termination

The services of permanent staff may be terminated after giving him one month's prior notice as per the terms of appointment / service agreement, if any, or payment of basic salary, in lieu thereof or for that matter clearance of

any pending salary or financial reimbursements and terminate him immediately after settlement of the same.

4.11. Staff Exit Policy

Processes are implemented to ensure that all access rights of users of VU's information systems are removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Processes and responsibilities are agreed upon and implemented to enable emergency suspension of a user's access when that access is considered a risk to the VU or its systems as defined. Staff fill their relieving checklist & get it signed by their reporting manager/Department Head before their last working day.

5. Enforcement

Any staff, contractor who is found to have violated the policies may be subject to disciplinary action, up to, including termination of employment or legal case against the staff, depending on the degree of the offense committed.

6. Distribution List

The following users have access to this policy:

All staff, contractor of Vishwakarma University

7. Acronyms / Definitions

VU: Here it refers to Vishwakarma University

STAFF, CONTRACTOR: here means any person employed for wages in or in connection with work of the VU or establishment to which the Policy applies.

IT AUTHORITY/SYSTEM ADMINISTRATOR: here means IT expert(s) appointed by the VU to monitor and support the running of the IT Department.

HR: here means the Human Resource(s) / Human Resource Department.

DEFAMATORY/LIBELLOUS: Anything injurious to the reputation of a person/VU.

EQUIPMENT: Equipment here means all the devices associated with the Computers(CPU, Monitor, Mouse, Printer, Server, Keyboards, Telephones,

Cables, RAM, Hard-disk, Laptops, Chargers, Pen-drives, CD's, DVD's, DVD Drives, Routers, Switches, Cameras, Fire alarms, Memory Stick, Flash Drives, Memory Cards)

COMPACT FLASH: It is a mass storage device format used in portable electronic devices.

CONFIDENTIAL BUSINESS INFORMATION: Confidential business information here means information which concerns or relates to the trade secrets, processes, operations, style of works, or apparatus, or to the production, sales, shipments, purchases, transfers, identification of customers, inventories, or amount or source of any income, profits, losses, or expenditures of any person, VU, partnership, corporation, or other VU, or other information of commercial value, the disclosure of which is likely to have the effect of either impairing the Commission's ability to obtain such information as is necessary to perform its statutory functions, or causing substantial harm to the competitive position of the person, VU, partnership, corporation, or other VU from which the information was obtained, unless the Commission is required by law to disclose such information. The term "confidential business information" includes "proprietary information" within the meaning of section 777(b) of the Tariff Act of 1930 (19 U.S.C. 1677f(b)). Nonnumeric characterizations of numerical confidential business information (e.g., discussion of trends) will be treated as confidential business information only at the request of the submitter for good cause shown.

QUARANTINE: To move an undesired file such as a virus-infected file or spyware to a folder that is not easily accessible by regular file management utilities. The quarantine option is available in antivirus software so that companies can keep a record of which users have been infected, where the file came from and to possibly send the virus to the antivirus vendor for inspection. Spyware blockers quarantine files so that they can be restored if required.

SECURITY PROTOCOL: A security protocol (cryptographic protocol or encryption protocol) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods.