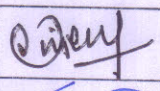
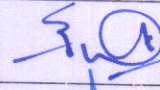
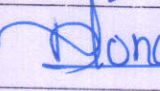


# **Standard Operating Procedure For Cyber Security Committee (CSC)**



## INDEX

Sr. No.	Description	Page No	
		From	To
1.	Objective	3	3
2.	Scope	4	4
3.	Committee Members	5	5
4.	Definitions	6	6
5.	Roles and Areas of Responsibility	7	8
6.	Principles for Cyber Security	9	14

Authority	Signature
Prepared by	 (U.M. Nair)
Approved by	 (Dr. S.H. Ghare)
Reviewed by	 (Dondhe D.W.)



**Objective :-**

The purpose of standard operating procedure in respect of Cyber Security Committee is to commit in safeguarding the confidentiality, integrity and availability of all physical and electronic information assets of the institution to ensure that regulatory, operational and contractual requirements are fulfilled.



**Scope:-**

The scope of this committee is to clearly define roles and responsibilities that are essential to the implementation and continuation of the GIT's Information Security Plan.

- Comply with requirements for confidentiality, integrity and availability for Gharda Institute of Technology's employees, students and other users.
- Establish controls for protecting GIT's information and information systems against theft, abuse and other forms of harm and loss.
- Motivate administrators and employees to maintain the responsibility for, ownership of and knowledge about information security, in order to minimize the risk of security incidents.
- Ensure the availability and reliability of the network infrastructure and the services supplied and operated by GIT.

**Committee Members:-****Responsible Person**

1. Mr. Vijesh M. Nair (Chairperson)
2. Mr. Vipul V. Shirgaonkar (System Admin)
3. Mr. Sameer S. Tathare
4. Mr. Pradeep P. Patil
5. Mr. Krunal P. Rane
6. Mr. Ketan. R. Kundiya



The Committee is responsible to do the following:

- Planning - Identify an annual work plan to achieve security goals and objectives consistent with the agency's strategic plan.
- Developing- Lead in the development of information security policies, standards, guidelines, processes, and procedures.
- Managing - Conduct risk assessments, manage incidents, provide internal and external reporting, involvement in security awareness education and training.
- Oversight - Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements (e.g., laws, regulations, statutes, state policy, etc.).

### Definitions:

**Data Classification** - In the context of information security, it is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization.

**University Data** - All data or information owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked.

**Information System**- Any electronic system that stores, processes, or transmits information.

**Information Assets**- Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the University

**Principle of Least Privilege**- Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.



**Principle of Separation of Duties-** Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.

### **Roles and Areas of Responsibility:**

The administration has the overall responsibility for managing Gharda Institute of Technology's values in an effective and satisfactory manner according to current laws, requirements and contracts.

The Principal/Trustee has the overall responsibility for information security at GIT network, including information security regarding personnel and IT security.

#### **5.1.1 Owner of the security policy**

The Principal/Trustee is the owner of the security policy (this document). The Chairman delegates the responsibility for security-related documentation to the CSC (Cyber Security Committee). All policy changes must be approved and signed by the governing council in consultation with CSC.

#### **5.1.2 Cyber Security Committee (CSC)**

The Cyber Security Committee (CSC) holds the primary responsibility for ensuring the information security at Gharda Institute of Technology's.

#### **5.1.3 System administrators**

System administrators are persons administrating GIT network's information systems and the information entrusted to the institution by other parties. Each type of information and system may have one or more dedicated system administrators. These are responsible for protecting the information, including implementing systems for access control to safeguard confidentiality, and carry out backup procedures to ensure that critical information is not lost. They will further implement, run and maintain the security systems in accordance with the security policy.



#### **5.1.4 Users**

Employees and students are responsible for getting acquainted and with GIT's IT rules and regulations. Queries regarding the administration of various types of information should be posed to the system owner of the relevant information, or to the system administrator.

#### **5.1.5 Consultants and contractual partners**

Contractual partners and contracted consultants must sign a confidentiality agreement prior to accessing sensitive information. The System administrator is responsible for ensuring that this is implemented.

### **Principles for Cyber Security:**

#### **3.1 Risk management**

1. GIT CSC should continuously assess the risk and evaluate the need for protective measures. Measures must be evaluated based on institute's role as an establishment for education and research and with regards to efficiency, cost and practical feasibility.
2. An overall risk assessment of the information systems should be performed annually.
3. Risk assessments must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.
4. Risk assessments are to be carried out when implementing changes impacting information security. Recognized methods of assessing risks should be employed, such as use of any physical firewalls.
5. The CSC is responsible for ensuring that the risk management processes at college are coordinated in accordance with the policy.



6. The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.
7. Risk management is to be carried out according to criteria approved by the management in consulting with CSC.

### **3.2 Information security policy**

1. The Principal/Trustee shall ensure that the information security policy, as well as guidelines and standards, are utilized and acted upon.
2. The security policy shall be reviewed and updated annually or as and when necessary, in accordance with principles and emergencies.
3. All important changes to GIT network's activities, and other external changes related to the threat level, should result in a revision of the policy and the guidelines relevant to the information security.

### **3.3 Security organization**

Security responsibility is distributed as follows:

1. Each department and section is responsible for implementing the unit's information security. Each HOD must appoint separate cyber security administrators.
2. The administration department has the primary responsibility for the information security in connection with the student registry and other student related information.
3. The IT System Admin has executive responsibility for information security in connection with IT systems and infrastructure.
4. The HR has executive responsibility for information security according to the Personal Data Act and is the controller on a daily basis of the personal information of the employees.



5. The Dean for Academic Affairs and Research Administration has executive responsibility for research related personal information.
6. The institute's information security will be revised on a regular basis, through internal control and at need, with assistance from an external IT auditor.

The security forum (CSC) has the following responsibilities, among others:

- Review and recommend information security policy and accompanying documentation and general distribution of responsibility.
- Monitor substantial changes of threats against the information assets of the organization.
- Review and monitor reported security incidents.
- Authorize initiatives to strengthen information security.

### 3.4 Classification and control of assets

1. "Assets" include both information assets and physical assets.
2. Information and infrastructure should be classified according to security level and access control.

#### ❖ Sensitive

Information of a sensitive variety where unauthorized access (including internally) may lead to considerable damage for individuals, the university college or their interests.

#### ❖ Internal

Information which may harm a specific department or be inappropriate for a third party to gain knowledge of. The System owner decides who may access and how to implement that access.



❖ Open

Other information is open.

**3.5 Monitoring of system access and usage**

1. Access and use of IT systems should be logged and monitored in order to detect unauthorized information processing activities.
2. Usage and decisions is traceable to a specific entity, e.g. a person or a specific system.
3. The System Admin should register substantial disruptions and irregularities of system operations, along with potential causes of the errors.
4. Capacity, uptime and quality of the IT systems and networks should be sufficiently monitored in order to ensure reliable operation and availability.

**3.6 Access control****3.6.1 User administration and responsibility**

1. Users accessing systems must be authenticated according to guidelines.
2. Users should have unique combinations of usernames and passwords.
3. Users are responsible for any usage of their usernames and passwords. Users should keep their passwords confidential and not disclose them unless explicitly authorized by the CSC.

**3.6.2 Access control/Authorization**

1. Access to information systems should be authorized by immediate superiors (HOD) in accordance with the system owner directives. This includes access rights, including accompanying privileges.



2. Authorizations should only be granted on a "need to know" basis, and regulated according to role.
3. The immediate superior should alert the system administrator about granting access and changes in accordance with the directives from the system owner.
4. Roles and responsibilities with accompanying access rights should be described based on the following classifications.
  - Internal (several roles)
  - External (several roles)
  - Student
  - Public
  - Others

### 3.6.3 Network access control

1. The System Admin is responsible for ensuring that network access is granted in accordance with access policy.
2. Users should only have access to the services they are authorized for.
3. The access to privileged accounts and sensitive areas should be restricted.
4. Users should be prevented from accessing unauthorized information.



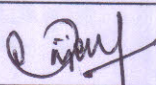
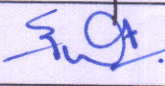

### 3.7 Compliance

#### 3.7.1 Compliance with security policy

1. All employees must comply with the Information security policy and guidelines. Enforcement is the responsibility of line management. Students must comply with IT regulations.
2. Employees and students should be aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.

#### 3.7.2 Controls and audits

1. Audits should be planned and arranged with the involved parties in order to minimize the risk of disturbing the activities of the institute.

Prepared By	 (V.M. Nair)
Approved By	 (Dr. S.H. Ghavate)
Principal	 (Dr. S.H. Ghavate)
Registrar	