Information Security Policy

Version: 1.0

May 5, 2020

1. Table of Contents

1. Table of Contents 2
2. Document Information 3
2.1. Approval Document 3
2.2. Document History 4
3. Purpose 5
4. Scope 5
5. Clause Reference 5
6. Policy Detail 6

2. Document Information

2.1. Approval Document

Document Name	Information Security Policy
Document Code	ITS-POL-003
Classification	Policy
Author	Owais Ahmed
Reviewer	Muhammad Saad Ullah Khan
Approver	Muhammad Saad Ullah Khan
Current Version	1.0
Release Date	May 5, 2020

2.2. Document History

Version Changed	Change Description	Change Approver	Approval Date & Method

3. Purpose

The primary purpose of this Information Security Policy is to promote business continuity, and to protect University and client information assets by minimizing the potential for security incidents, whether internal or external, deliberate or accidental.

4. Scope

This policy document applies to ITS department.

5. Clause Reference

- 6.6.1 Information security policy

6. Policy Detail

This is the policy of ITS department at the Sybrid to create, maintain and continually improve the Information Security and to adhere to best practices in compliance with best practices required for service delivery and information security needs of the customer.

ITS department at the Sybrid works within the framework of the Local Government, while fulfilling the contractual obligation of the client. This is to ensure protection of its information assets from all threats – internal or external, deliberate or accidental and natural disasters.

Furthermore, to achieve this objective ITS department at the Sybrid will ensure the following:

- Business requirements for availability of information and systems are met.
- Confidentiality, integrity, and Availability of information is maintained throughout the process flow.
- All corporate assets (tangible/intangible) are located in a physically and logically secure environment.
- Risks to all corporate assets (tangible/intangible) are assessed and against all risks appropriate contingency and mitigation plans are defined.
- Human resources are provided with conducive work environment, free from safety hazards.
- Physical, Logical and Remote access to all the corporate assets (tangible/intangible), information and physical locations is monitored and controlled.
- Service continuity plans are established, maintained, and tested and periodically and updated as needed.

This policy has been approved by the company management and shall be reviewed by the management in annual management review meeting.