Policy:	**Data Security**		
Code:	**07HS03**		
Reviewed/ Revised:	**28/07/2022**	Date of Next Review:	**February 2024**
Policy Owner:	**IT Manager**		
Target audience:	**EAHM Student, Staff and Faculty**		

PURPOSE:
The purpose of this policy is to provide guidelines in securing data stored and shared within EAHM.

SCOPE:
The policy clarifies the controls placed to ensure Data security for all EAHM Students, Staff and Faculty, excluding external guests as they use a separate network from the rest ensuring no possible breach.

DEFINITIONS:
In this context, **"student"** includes full- and part-time degree students and exchange students, as well as participants in short courses and professional development. Access rights to computing and network facilities differ with the type of student but the guidelines for use are the same for all users.

LMS: an acronym for Learning Management System
ERP: is an acronym for Enterprise Resource Planning and it is the platform that unifies our HR, Finance and procurement systems in 1 platform.

POLICY STATEMENT:
EAHM provides and ensures that proper data protection and security controls and procedures are in place to avoid potential financial, reputational and information risks

RESPONSIBILITY:
IT department is responsible for formulating and implementing data security procedures with the objective to ensure the protection of important and sensitive institutional data and IT infrastructure.

The IT Manager is responsible to monitor and update the policy as and when required.

IMPLEMENTATION OF THE POLICY:

1. **General Policy of Data Security**
   The following broad principles are followed for ensuring data security:
   - limits internal access to education records and other data based on role of the user
   - ensures security protocols are updated from time to time
   - builds user awareness especially in times when threats from viruses and malware are anticipated, that includes sending out warnings and directions on how to react when receiving viruses and attacks.
   - Users maintains reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of data.

2. **Adopted Measures**
   The specific security measures adopted by IT department include the following:
   - A Firewall is in place to block unauthorized traffic and networking hardware is all password protected.

- Passwords for public PC's are being changed every academic year to protect it from leaking to unauthorized users.
- Web & Network Threat protection kept in place to prevent attacks from malware, risky file types and websites, and malicious network traffic.
- Anti-virus is installed on all computers (Endpoint Security blocks network activity from the attacking computer).
- Users with personal computers are limited to Wi-Fi and relevant services.
- Network accounts and permissions are implemented.
- Microsoft Active Directory Controls Network Access.
- Shared storage only to permitted staff.
- Data is remotely backed up with security in place.
- No applications can be installed or removed without an IT administrator password provided.
- Public websites protected by secure socket layers.
- IT infrastructure, especially server rooms have fireproof doors and access is limited to only few authorized IT staff.

3. Data Storage and Backup Policy

Information Technology (IT) Department follows various applications for data storage and its backup. The details of data storage and its backup faculty are as follows:

4. Storage

a. EAHM provides limited disk-based storage space for individual faculty and staff, for course-related materials, and for departmental materials.
b. Digital copies of Faculty and Staff files are stored on File Server
c. Course related materials are stored in Cloud based LMS.
d. All employees will login to the file server through user ID and password.

5. Data Backup

a. Backup is setup during installation of Operating System in a PC. As an additional security measure.
b. Files are automatically being backed up to backup tapes that are available in premises, then in monthly basis stored off-site as a disaster prevention plan
c. IT department is responsible to maintain and manage backups for servers in a redundant way to not lose any data if any of the backup disks fail. Virtual servers are on RAID 1 mode, physical servers are on RAID 6

6. Recovery Plan

Following Recovery plan for servers are maintained:

Key business process	**Backup strategy**
IT Operations Hardware	Contractual plan with replacement
LMS	On-premises and being backed up every day, week, and month to backup tapes
Mail Office 365	Fully mirrored recovery from cloud
ERP	Fully mirrored recovery from cloud
Finance	Fully mirrored recovery from cloud
Website	Fully mirrored recovery from cloud
File Server	Daily, weekly, and monthly backup of data is being stored in backup tapes

VIOLATION OF THE POLICY
Violation of the Data Protection Policy by a member of the EAHM Students, Staff or Faculty will result in disciplinary actions as per the EAHM **06ST13 Student Discipline** for students or the HR policy for staff and faculty.

ASSOCIATED DOCUMENTS:
- Risk Management Register
- 06ST13 Student Discipline
- HR Policy

MENTIONS:
- Catalogue
- Student Handbook
- EAHM Policy and Procedures handbook

DATE OF NEXT REVIEW:
This document should be reviewed by **February 2024.**

POLICY APPROVALS RECORD

Policy Name:	**Data Security**		
Policy Code:	**07HS03**	Formerly:	NA
Date of first approval:	**28/07/2022**		

Reviewed/ Updated	Details of Amendment