IT POLICY

1. PURPOSE

AGE recognizes the vital role information technology plays in the AGE objectives and related administrative activities, as well as the importance in an academic environment of protecting information in all forms. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the Institute, an increased effort must be made to protect the information and the technology resources that support it.

2. INTRODUCTION

AGE IT policies are included here, that include the use of information technology, and IT policies for students and AGE staff. The main IT provider for AGE will be Schneide Solutions Co., India. It will be ensured by Schneide that dedicated servers are allocated to AGE, the Server Access Controls should be well defined, and data storage, back-up procedures and security monitoring processes should be explicitly laid down by the company. The SLAs with service Providers, including guarantees should be agreed upon in the agreements. In particular, the Learning Management System (LMS) and the Customer Management System (CRM) will be designed for AGE in consultation with the Group Management, which should help authorized access users to feed in staff and student data, as well as all academic materials and resources for easy access of students. Every access control for any authorized person should have a unique username and password for easy access. The process flow right from students' information capture, to their recruitment and till the culmination of the programme should be automated for ease of operations and control.

3. IT ACCESS & PROTECTION

This policy applies to the electronic access given to faculties, staff and students, as well as the responsibilities of different staff members to ensure protection of system and data in all eventualities. Some of these are enumerated below.

- **System Protection, Maintenance and Management**. All Schneide and AGE systems require ongoing maintenance and inspection to ensure that they are operating properly. It also has to be ensured that the systems are protected against threats such as attacks, malware, and viruses, as well as the integrity and security of information is always protected. IT Company Schneide will ensure upkeep and maintenance of equipment, systems protection, including data storage protection and managing disaster recovery. At the Institutes level, the programme Course Administrator will be responsible for the day to day operations, including students' technical or other IT issues, wherein any student's IT concerns will be resolved by the programme Course Administrator.

- **Business Continuity**. In case of any major disruption in IT resources access to staff and students, business continuity will be maintained by employing the back-up servers within one day by the IT Company Schneide. All data stored on main servers should be accessible to all concerned users within this time period. At Institutes level, user electronic information should be accessible for the purpose of ensuring continuity in business operations. This need can arise, for example, if an employee who typically has access to the files in question is unavailable due to illness or vacation.

- **Safety Matters**. The Institute should be able to access user electronic information to deal with exigent situations presenting threats to the safety of the campus or to the life, health, or safety of any person. This will be the responsibility of the Admin staff member earmarked for AGE, who should be able to access all such information.

- **Legal Process and Litigation**. The Institute should be able to access user electronic information in connection with threatened or pending litigation instituted by a staff member, a student or any other outside person against AGE, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes through the available electronic information.

- **Internal Investigations of Misconduct**. The Institute may access user electronic information in connection with investigations of misconduct by staff members or students of the Institute, but only when the authorizing person, after weighing the need for access with other AGE values, has determined that such investigation would advance a legitimate validity with sufficient basis for seeking such access. All such decisions to access user electronic information are subject to review by the Disciplinary Committee.

4. CLASSES OF IT RESOURCE USERS

The information technology resources owned and managed by AGE will be used by two distinct classes of users:

1. **Employees.** These include individuals who are regular AGE employees, as well as visiting faculty, “adjuncts,” and other persons who have been officially sanctioned such access. These users gain access to AGE information technology resources by virtue of their employment or sanctioned affiliations.

2. **Students.** These include individuals registered as full - or part-time students at AGE. These users gain access to AGE information technology resources as part of the service package the Institute provides to registered students.

5. GUIDELINES FOR USE OF IT RESOURCES

The following guidelines are given below for ethical reasons, so that the IT resources are not misused under such circumstances which are given below. The list covers some important salient examples, but is not an exhaustive one, and can cover under its jurisdiction any such similar examples as given below:

1. Using resources for derogatory, racially offensive, sexually offensive, harassing, threatening, or discriminatory purposes.

2. Downloading, installing, or running malicious applications and programmes which are harmful for the established IT systems.

3. Unauthorized use of computers and User IDs, or use of User IDs for purpose(s) other than those for which they have been issued.

4. Accessing computers, computer software, computer data or information, or networks without proper authorization, or trying to hack into systems using unauthorized access resources.

5. Circumventing or attempting to circumvent normal resource limits laid down for members who are allowed access, including logon procedures, or security regulations.

6. Sending fraudulent e-mails/ messages, breaking into another user's e-mail account, or reading someone else's e-mail/ message without his or her permission, unless specifically authorized to do so.

7. Sending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information, fraudulent submission of electronic purchase requisitions/ vouchers, or fraudulent electronic authorization of purchase requisitions/ vouchers.

8. Violating any legal software license agreement or copyright, including copying or redistributing copyrighted computer software or data without proper, recorded authorization.

9. Taking advantage of another user's inexperience or negligence to gain access to any system account, data, software, or file which would not otherwise be accessible.

10. Disclosing proprietary information, software, printed output, or magnetic media without the explicit permission of AGE.

Note: IT Infrastructure set up, maintenance and operational aspects are given at Appendix.

Appendix

1. IT INFRASTRUCTURE

Dedicated Servers Schneide hosts all applications and websites in its fully managed dedicated servers managed through the server providers Znetlive in Jaipur, India. The dedicated server is hosted in the Hetzner Online GMBH, Gunzenhausen, Germany Data Center; this data center is certified in accordance with DIN ISO/IEC 27001.

Server I
Dedicated Server - Germany (Intel Core i7-6700 Quad-Core Skylake - 3.4 GHz/Core)
Processor: Intel® Core™ i7-6700 Quad-Core Skylake
RAM: 64 GB DDR4
Hard Drive: 500 GB SSD
Second Hard Drive: 500 GB SSD
Disk Controller: RAID 1
Port Speed: 1000 Mbps
Allocated NAS: 100 GB NAS

Managed – Fully Managed
Operating System: Windows Server 2012 R2 Standard Edition
Control Panel: Plesk Web Host Edition
Database Software: Microsoft SQL Server 2012 Express
Mail Server Software: SmarterMail Pro - 250

Server II
Cloud Server – Microsoft Azure
Size - Standard B4ms (4 vcpus, 16 GiB memory)
Operating System - Windows (Windows Server 2016 Data center)
Hard Drive - 256 GiB (Standard HDD)
Location – India Data center
Managed – Fully Managed

Server III

1. **EC2**

Cloud Server – AWS
Size - Standard (2 vcpus, 8 GiB memory)
Operating System - ubuntu/images/hvm-ssd/ubuntu-bionic-18.04-amd64-server**)** 3.7.173.255
Hard Drive - 50 GiB
Location – ap-south-1a **Managed**
– Fully Managed

2. **RDS**

Cloud Server – AWS
Size - db.t2.small
Operating System - RDS
Hard Drive - 50 GiB
Location – ap-south-1a **Managed**
– Fully Managed

3. **AWS S3 unlimited Bucket**
Unlimited storage and region independent

2. SERVER ACCESS CONTROLS

Access to the servers are restricted to 2 users only as follows:

1. Super user who has access to server, network and all database, websites, this privilege is given only to the Director Schneide solutions.

2. Server Administrator has access to manage the network, DNS and security related monitoring and control. This access is given to the designated server administrator of the server provider

3. Servers can remotely be accessed only through VPN (Virtual Private Network) which is restricted to the super user.

All administrator passwords are generated as a complex password and are forcefully changed every month.

3. DATA STORAGE. The following data are captured and stored in the server:

1. All applications (LMS, CRM) data are stored in Microsoft SQL server as database schema objects.
2. The application user files like assignments and other reference materials are stored in physical disk drive (RAID 1) under respective applications.
3. Website data stored as database schema objects in MySQL.

4. BACKUP PROCEDURES

The backup software used to control the backup processes is Acronis cloud backup (https://www.acronis.com/en-in/). The Systems Support team (server providers) ensures that all backups are completed successfully and reviews the backup process on all servers daily. Logs are maintained to verify the amount of data backed up and the unsuccessful backup occurrences.

4.1 Daily Backups - Backup software is scheduled to run every day at 4:00AM IST, to capture all data from the previous day. This includes all database websites and website contents. The backed-up data is also moved to external Network Attached Storage (NAS). These backups will be retained for seven days, on eighth day it would be overwritten.

4.2 Data Mirroring – The hard drives in the servers are replicated using RAID 1 technology which provides data protection and disaster recovery.

5. SECURITY MONITORING

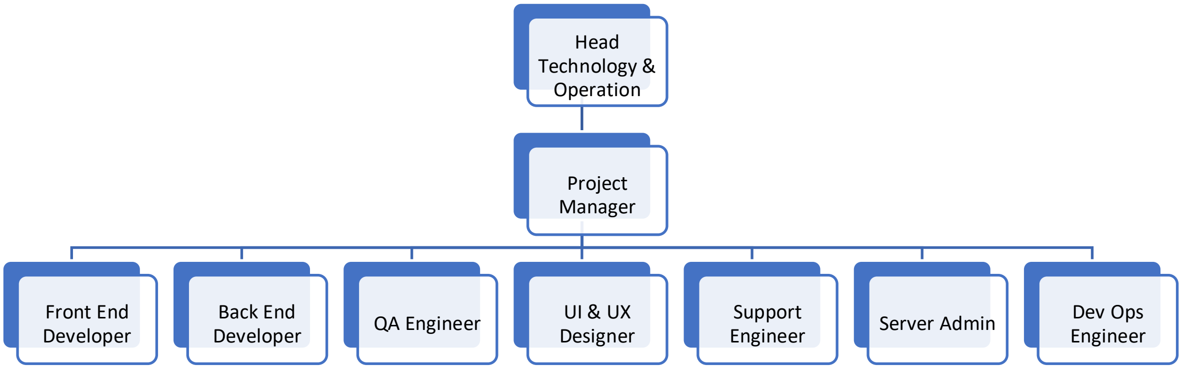
Anti-Spyware - All servers have an anti-spyware application installed this offers real-time protection to the target system

Following activities are regularly monitored by our designated administrator

- Intruder monitoring
- Security Patch updation

- Daily Backup monitoring
- Bandwidth monitoring
- Identify bottle necks
- Performance and fault monitoring
- IP backlisting monitoring
- Review failed login attempts and blocked IP
- Antivirus updation
- Quarantine management

6. ORGANISATIONAL STRUCTURE (AGE)



7. SERVICE LEVEL AGREEMENT (SLA)

SLA with ZNetlive (server provider) ZNetLive (server provider) guarantees 99.9% availability of its monitoring services and infrastructure for Managed Windows service along with the commitment to maintain services in proper operational condition. Severity 1 (S1) – System down impacting customer significantly Severity 2 (S2) – System functioning despite degraded performance

Severity 3 (S3) – Error not impacting the end customer.

The server provider agrees to adhere to the service response time as below:

The server provider agrees to adhere to the service response time as below

Severity	Log Time	Respond Time	Target time to update customer
S1	20 minutes	15 minutes	Every 1 hour
S2	40 minutes	30 minutes	Every 4 hours
S3	60 minutes	60 minutes	Every 8 hours
Change Request	30 minutes	2 hours	4 hours or upto completion of change request

8. HARDWARE REPLACEMENT OR UPGRADATION

Hardware Replacement:

ZNetLive guarantees that in the event of any hardware failure, the faulty hardware will be replaced within 6 hours of identifying the problem.

In case this guarantee is not met, ZNetLive will provide a credit of:

- 0% of the first month's invoice amount if the time period of upgradation from being scheduled is less than 6 hours.

- 10% of the first month's invoice amount if the time period of upgradation from being scheduled ranges between 6 to 12 hours.

- 20% of the first month's invoice amount if the time period of upgradation from being scheduled ranges between 12 to 18 hours.

- 30% of the first month's invoice amount if the time period of upgradation from being scheduled ranges between 18 to 24 hours.

- 50% of the first month's invoice amount if the time of upgradation from being scheduled exceeds 24 hours.

Dedicated server hardware covered under this guarantee includes processor(s), hard drive(s),

RAM, network card(s), motherboard and all other hardware that is related directly to the server offered in the plan.

9. NETWORK UPTIME SERVICE LEVEL AGREEMENT

ZNetLive guarantees 99.9% network uptime to customers. 99.9% Network uptime may be defined as the availability of the network from the internet across the globe 99.9% of the time.

Network downtime may be defined as ZNetLive's network unavailability (excluding maintenance period) for continuous 15 minutes of time with no internet traffic to the server as verified by the support team at ZNetLive. Downtime is determined from the time when the affected customer raises a support ticket to the time ZNetLive considers the problem as resolved.

In an unlikely event of downtime, ZNetLive will compensate customers as given below:

- If Network Uptime is less than 99.00%, the customer will be provided 5% of the first month's invoice amount
- If Network Uptime is less than 98.5%, the customer will be provided 10% of the first month's invoice amount
- If Network Uptime is less than 98.00%, the customer will be provided 15% of the first month's invoice amount
- If Network Uptime is less than 97.50%, the customer will be provided 20% of the first month's invoice amount
- If Network Uptime is less than 97.00%, the customer will be provided 30% of the first month's invoice amount Severity Log Time Respond Time Target time to update customer

S1 20 minutes 15 minutes Every 1 hour

S2 40 minutes 30 minutes Every 4 hours S3

60 minutes 60 minutes Every 8 hours

Change Request

30 minutes 2 hours 4 hours or up to completion of change request 112

•If Network Uptime is less than 96.5%, the customer will be provided 40% of the first month's invoice amount

•If Network Uptime is less than 96.00%, the customer will be provided 50% of the first month's invoice amount

•If Network Uptime is less than 95.50%, the customer will be provided 60% of the first month's invoice amount

•If Network Uptime is less than 95.00%, the customer will be provided 60% of the first month's invoice amount

• If Network Uptime is less than 94.0%, the customer will be provided 100% of the first month's invoice amount

10. FAQS

Q 1: Is there an IT helpdesk?

A 1: Yes, we allocated 2 dedicated support personnel to attend all IT related support issues raise from the applications (LMS/CRM). Any change requests/issues which warrants change in the application program are directed to the development team.

Q 2: If VLE is down how is it backed up?

A 2: The contents of the LMS are maintained as database schema objects in Microsoft SQL Server. Each application has separate database with different access privileges. The backup of database is scheduled to execute every day night. One copy is stored in the cloud and another is stored in the NAS drive.

Q 3: Where are students records stored?

A 3: Students assignments files and supporting documents (which are uploaded by the student) are stored in the hard disk drive of the dedicated server. Which is a mirrored disk (RAID 1 type).

Q 4: What is the disaster recovery plan? If IT systems went down what would we do?

A 4: We use two dedicated servers with almost same configuration. All data including the database, application files, website contents are backed up daily and are stored in two locations (cloud and NAS).

In case of any system failure the data and the application can be restored in other server within few hours (depends on the volume of data).

Q5: How do we store data and how do we back it up, including whose responsibility is it to organize the back up?

A 5: Refer Q3 for the details of data storage. Backup is scheduled using the backup tool, the backup log has been monitored by the Project Manager – Schneide solutions.