Information Technology - Disaster Recovery

1. Background & Objective

A disaster recovery plan for information technology is very crucial for any organization, no matter how big or small. It helps us by developing an action plan for unplanned disruptions. The most important advantage of having a disaster recovery plan is that we will gain the support and trust from our customers, stakeholders, and law enforcement.

We must ensure that our business continues to operate in the event of an incident. It is important to plan for everything and to establish priorities that can be used to identify and visualize how we can recover from a catastrophic business loss. How will we address the situation if data is lost because of a breach? This policy calls for the creation of action teams to implement our contingency plan.

2. Scope

This plan will focus exclusively on the recovery of systems and technologies that are controlled directly by the Information Technology Department and are vital for business continuity. This encompasses the following significant areas:

- Datacenter facility
- User directory services
- On premise virtualization server, storage, & file server
- On-premises enterprise application such as ERP, GAIS (GA System), Legal System
- On-premises services such as printing services, attendance system, CCTV, etc.

- Computer desktop and its equipment, computer laboratory, and classrooms
- Telecommunications and data network including telephony, LAN & WAN connectivity, core routing and firewall services
- The recovery of numerous crucial application which are hosted in the cloud (outside the university) are not covered by this document, but this strategy will address the integration and connectivity with these application / services. This category contains the following major services:
- Academic system (ACADIS, ARIS, AHRS, RMS)
- Campus back-office system (ERP, GAIS, SPS, FMS, LMS, DMS, HRIS)
- Library System
- Learning Management System
- Email and Microsoft Office 365 Family Apps

This plan addresses all phases of any IT-related disaster that may occur at Sampoerna University.

3. Assumption

The following assumptions underpin this disaster response and recovery plan:

Once a disaster is declared for an incident covered by this plan, the recovery effort will be given based on the necessary priority. Necessary resources and support as described in the IT Disaster Recovery Plan shall be made available.

The safety of faculty, staff, and students is the most important thing, and concerns about hardware, software, and other recovery needs will be secondary.

Depending on the disaster severity, every campus department/unit may be required to alter their operations to adapt to changes in computer availability, system performance, and or physical location until a complete recovery occurs.

The Information Technology Department will encourage other units/departments to develop business continuity plans and contingency plans for their operations, which will encompass periods of time without IT systems.

4. Roles & Responsibilities

4.1. Disaster Management Team

The Disaster Management Team is in charge of giving overall guidance for the university's recovery efforts. It determines the scope of the harm and initiates the organization recovery. The primary function of this team is to oversee and direct the recovery process. The Disaster Management Team will have the following responsibilities:

- Assessing the scope of the problem and its possible consequences, as well as initiating disaster recovery procedures.
- Managing recovery teams; supervising recovery operations; updating top management about the disaster, recovery status, and related issues.
- Managing and controlling emergency expenses and costs; speeding expenditure approvals for other teams.
- Liaising with other department managers as necessary to activate business continuity plan of its department while the technology is being recovered.

The Disaster Management Team is led by Vice Rector of Administration, Resources, and Operations (VRARO). The Disaster Management Team Leader is in charge of determining whether the circumstances require for disaster recovery procedures to be implemented. If the Disaster Management Team Leader determines that it does, all procedures and the organization established in this document take effect for the duration of the crisis.

Disaster Management Team Members are:

1. Vice Rector of Administrations, Resources, and Operations
2. Finance & Operation Manager
3. Information Technology Manager
4. Human Resources Manager
5. Head of Academic Operations

4.2. Recovery Coordinator

The Disaster Management Team will have two coordination roles that will report to them. They are the disaster recovery coordinator and the business recovery coordinator.

A Disaster Recovery Coordinator serves as the primary point of contact for the datacenter, infrastructure, and server recovery team; the telecommunications, network, and internet services recovery team; application & enterprise system recovery team; and desktop, lab, classroom, and other IT facilities recovery team. He/she will be responsible for disaster notification, problem resolution, and damage control.

The Business Recovery Coordinator will create and update Business Recovery Plans, as well as coordinate recovery efforts and notification in every business unit within the university.

4.3. Datacenter Facility, Infrastructure, and Server Recovery Team

The Datacenter facility, Infrastructure, and Server Recovery Team is made up of members from the Information Technology department who are responsible for supporting the university's datacenter and central computing environment, which houses all central IT services, Network Operations Center, and other central computing resources. Additionally, the team is in charge for network infrastructure support for the university, which includes User Directory, DNS, DHCP, file servers, virtualization sever, network storage, and web server.

This working group's major responsibility is to restore the existing datacenter facility, servers, and network infrastructure to their most current pre-disaster configuration in circumstances of significant data and operational loss. In less serious circumstances, the team is responsible for recovering the system to a functional state as a result of hardware failures or other unexpected conditions that could result in impaired operation or performance.

The team should be activated in the situation that any component of the datacenter facility, server, and network infrastructure encounters a severe disruption in the services as a result of unexpected circumstances and needs recovery efforts beyond those required on a daily basis. In the case of off-premises services, the team will organize the recovery process with the external service providers.

4.4. Telecommunications, Network, and Internet Services Recovery Team

The Telecommunications, Network, and Internet Services Recovery Team is made up of members from the Information Technology department who are responsible for maintaining the university's voice and data networks, which include PABX system, structure cabling system, firewall services, switches, and routers. This working group's major responsibility is to restore our voice and data networks, as well as Internet services, to their most current pre-disaster configuration in the event of significant operational loss. In less serious circumstances, the team is in charge for restoring Internet services, and voice and data network to a functional state as a result of any breakdowns or other unforeseen circumstance that may result in impaired performance or operation.

The team should be activated if some aspect of the data or voice networks suffer a severe interruption in the services as a result of unexpected circumstances and needs recovery efforts beyond those required on a daily basis.

4.5. Application & Enterprise System Recovery Team

The Application & Enterprise Systems Recovery Team is made up of members from the Information Technology department who are responsible for supporting all applications and information systems utilized by the University for both academic and administrative supporting systems. This working group's major responsibility is to restore all modules and data in the applications to their most current pre-disaster configuration in circumstances of significant data or operational loss. In less serious circumstances, the team is responsible to restore the system to functional status as a result of network outages, hardware failures, or other occurrences that may impair system performance or operation.

The team should be activated in the event one or more academic or administrative supporting systems suffer a severe interruption in their services as a result of unexpected/unforeseen circumstances and needs recovery efforts beyond those required on a daily basis. In the case of off-premises application (such as SAAS/Software as a Service application) the team will organize the recovery process with the external service providers.

4.6. Desktop, Laboratory, Classroom, and Other IT Facilities Recovery Team

The Desktop, Laboratory, and Classroom Recovery Team is made up of members from the Information Technology department who are responsible for the maintenance of desktop hardware, client applications, classrooms, and labs. This working group's major responsibility is to restore SU's desktop computers, classrooms, and labs to functional condition. The team is not responsible for restoring any individual user's data that are stored in their desktop computer during the initial recovery procedure. Sampoerna University strongly advises all users to store their data in the cloud drive such as Microsoft One Drive, which can be readily downloaded and recovered at any time.

The team should be activated if there is a major interruption in desktop, lab, or classroom services as a consequence of unexpected/unforeseen situations that necessitate recovery efforts above what is normally seen on a day-to-day basis.

4.7. Communication Team

The Communications Team is made up of members from across departments such as Academic Operations, HR, and Marketing.

The Communication Team is responsible to obtain communication and information directives from the Disaster Management Team and communicate information during the phases of disaster and recovery to all employees, students, and other relevant external parties. Information that is made public must be managed and handled by Marketing. The following are some activities which are covered by the Communication Team:

- Liaising with the Disaster Management Team and Recovery Coordinator to obtain directives on the messages to be communicated.
- Updating employees on the schedule of the recovery progress.
- Informing students and or third parties of the recovery progress and any potential delays.
- Making statements to press / media if necessary.
- Assuring there are no miscommunications that may harm the reputation of the organization.

5. Recovery Preparations

The availability of all essential information to ensure that hardware, system/software, and data can be recovered to a state as near to "pre-disaster" condition as possible is a critical prerequisite for disaster recovery. This section specifically addresses backup strategies and service restoration as they apply to hardware configurations, operating systems, and applications.

5.1. Backup Strategy

Backup and recovery files are necessary to restore systems to their pre-disaster condition, containing the information and data that were resident on the system shortly before the disaster. Sampoerna University runs a daily backup for all systems (both of data and configuration) which are hosted in either our internal data center or cloud infrastructure provider. Due to a limitation of storage, we only keep seven days of backup retention.

In technical practice, only the servers in the datacenter are backed up; as a result, only data stored on these systems may be restored. In the case of a campus disaster that damages personal computers, the information stored on these computers will be exceedingly difficult or impossible to recover. Data Backup of individual computers is the responsibility of the users. The Information Technology department encourages and recommends all users to use network drives or cloud drives such as Microsoft One Drive to store all important files.

5.2. Service Restoration

It is critical to fully restore all systems, but a sound restoration process requires that certain systems be restored in a specified order. No more than one system can be restored concurrently. As a result, the Information Technology Department has examined and prioritized system recovery and procedures based on the existing infrastructure setup and configuration.

The priority of restoration is defined based on the university's business impact and the time period which departments can continue operating independently using the alternate techniques outlined in their department business continuity plans.

The list of prioritized systems below is available to help departments prepare their department business continuity strategies. The systems contain time intervals needed which campus units will be required to implement alternate methods of executing their routine business operations.

Priority 1

Priority 1 covers all data center equipment, hardware, system / software, and structure cabling needed to restore the university network and telecommunications infrastructure.

System	**Estimated Time to Recovery**
Datacenter facility	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Internet access and network connectivity	36 hours using backup spare Estimated 8-16 weeks for procuring new equipment/spare part
Server, storage, and virtualization infrastructure	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Authentication and authorization systems: AD, ADFS, CAS	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Remote connectivity and VPN services for users	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Telephony and voice system	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part

Priority 2

Priority 2 covers all critical systems and applications which are very important but do not provide infrastructure.

System	Estimated Time to Recovery
CCTV System	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Access card (security system) and attendance system	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Shared network drive	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Campus on-premises back-office application: Oracle ERP, FMS, SPS (billing system), DMS	36 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Campus SAAS or cloud hosted back-office application: HR System	Services are hosted in the cloud provider and will be unaffected by incident in campus.
Cloud hosted academic application: Canvas LMS, ACADIS, ARIS, Online Test System	36 hours for switching to another provider Services are hosted in the cloud provider and will be unaffected by incident in campus.
SAAS: Microsoft Office365 Apps (including email), Canvas LMS	Following Provider SLA Services are hosted in the cloud provider and will be unaffected by incident in campus.

Priority 3

Priority 3 covers all critical equipment, systems, and applications but does not have an impact on the entire university.

System	Estimated Time to Recovery
Campus on-premises back-office application: GAIS, Legal System, RQMS	72 hours using backup spare Estimated 4-8 weeks for procuring new equipment/spare part
Campus SAAS or cloud hosted back-office application: Salesforce CRM	Following Provider SLA Services are hosted in the cloud provider and will be unaffected by incident in campus.
Campus SAAS or cloud hosted academic application: RMS, AHRS, OJS, LIBIS	72 hours for switching to another provider Services are hosted in the cloud provider and will be unaffected by incident in campus.
Campus and other websites portal	72 hours for switching to another provider Services are hosted in the cloud provider and will be unaffected by incident in campus.

Priority 4

Priority 4 covers all equipment, systems, and applications that may not be functionally recovered until normal operations are resumed.

System	Estimated Time to Recovery
Printer and copier services	10 working days using backup spare Estimated 8-16 weeks for procuring new equipment/spare part
Desktop, Lab, and Classroom Technology	10 working days using backup spare Estimated 8-16 weeks for procuring new equipment/spare part
Library Security System (RFID & self-check system)	10 working days using backup spare Estimated 8-16 weeks for procuring new equipment/spare part
Development server (sandbox application)	10 working days using backup spare

	Estimated 8-16 weeks for procuring new equipment/spare part
System to provide interfacing with external system such as SISTER, Neo Feeder, etc.	10 working days using backup spare Estimated 8-16 weeks for procuring new equipment/spare part

5.3. Recovery and Reference Documents

All procedures, guidelines, contracts, and other confidential documentation needed for technical disaster recovery are maintained securely and are accessible at any time and from any location by personnel or teams in the Information Technology Department who are in charge of maintaining related devices, systems, or applications. All recovery documents are checked, revised, and uploaded on a regular basis to onsite and offsite (cloud) document storage facilities.

6. Disaster Declaration

The most crucial and challenging aspect of disaster response is efficiently deploying the appropriate individuals during the plan's activation. Individuals are taking on new tasks and duties as a result of the disruption of typical processes, and they must adjust to changing conditions fast.

In the event of a disaster, the Disaster Management Team Leader determines whether to state a disaster and enable the Disaster Recovery Plan, as well as which recovery scenario will be executed. The Recovery Teams next carry out the stated recovery actions based on the set priority system list and act in accordance with each team's responsibilities, as outlined in this Disaster Recovery Plan. Each team will use its own procedures, disaster recovery knowledge, technical experience, and recovery tools to return their systems to operational status as quickly and accurately as possible. While various teams may be able to recover in parallel, the data center and network/telecommunications infrastructure will usually be given the top priority, as most other systems will not be fully functioning until these areas are restored.

The Disaster Management Team will decide the response in the event of a system disruption based on the levels of disasters and emergencies as described below:

Minor Incident

Minor incidents are more common, and their consequences are frequently limited to a subset of essential business processes or areas. Business units that rely on these processes can continue to operate for a limited period of time when a single component, system, or service fails. In this situation, the objective of the recovery process is to restore hardware (server, network device, or other equipment) or applications / systems to its normal function. Examples of this incident category include a temporary disruption of network access or connectivity, phone service or voice communications, a server in the datacenter, web application / portal access, or access to any cloud-based services.

Medium Incident

Medium incident occurrences are less common than minor incidents but have a higher impact. These incidents have a significant impact on areas of the university, interfere the normal operation of some but not all critical business units, and are typically the consequence of many systems and equipment failing catastrophically. In this situation, the objective of the recovery process is to reestablish minimum crucial application functionality, which may require relocating impacted applications / systems to alternate equipment. Examples of this incident category include the failure of major university administrative and academic systems, water entry or leakage that displaces or disturbs data center equipment and servers, the loss of internet or communication line such as FO cut, or electrical outages lasting more than 4 hours.

Major Incident

A major incident has a small chance of happening, but it has a serious influence. These incidents cause the inaccessibility or breakdown of most systems and equipment, disrupting the normal operation of all important business activities. In this situation, an authorized person (Disaster Management Team Leader) would declare an emergency and activate the Disaster Recovery Plan right away.

The objective of the recovery process is to restore minimum crucial application functionality either at the main or at the alternate facility as soon as possible. If the restoration timeframe is insufficient

(example: more than one month), temporary or new production facilities may need to be bought or leased. Examples of this incident category include floods, fires, earthquakes, and sabotage.