CORVINUS UNIVERSITY of BUDAPEST	**PROVISIONS OF THE EXECUTIVE COMMITTEE**	**1/2024.** Version number: **00.**

IT BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

Person responsible for professional aspects:	**Tibor Sopronyi**	Head of IT
Person responsible for professional review:	**Balázs Locsmándi**	Data Protection Officer
Legal aspects checked by:	**Zsuzsanna Borbás**	Head of Economic Law, Procurement, Labour Law Services
Decision-making body:	**Executive Committee**	
Person responsible for editing and publishing the text:	**Anikó Erős**	Higher Education Expert

Version Number	Date of publication	Effective date	Version tracking
00.	01. 10. 2024	01. 10. 2024	**Publication** Resolution No. VB-8/2024. (30 September)

CORVINUS UNIVERSITY of BUDAPEST	**PROVISIONS OF THE EXECUTIVE COMMITTEE**	**1/2024.** Version number: **00.**
IT BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN		

Table of contents

IT BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

Purpose of the provision

1. §

(1) The purpose of the IT Service Continuity Plan is to define the risks of potential IT-related disasters, the elements and steps to be taken to address them, in order to ensure the continuous availability of the IT/information systems of Corvinus University of Budapest (hereinafter: University).

(2) The fundamental objective for the University's business continuity is to ensure that in the event of a critical IT resource/function failure - a so-called IT disaster situation (hereinafter referred to as IT disaster situation or incident) - IT services are restored as soon as possible, either by using workarounds or by using bypass solutions, but in any case within the timeframe expected by the individual business area data and process owners.

(3) On the one hand, the provision defines the preparedness tasks to be carried out during normal operations, the assessment, planning, control and repair tasks to ensure that normal operations are restored as soon as possible after a disaster. On the other hand, it defines the human and material conditions for recovery.

(4) The document will help you in the event of an IT disaster situation in Informatika:

- the ability to react quickly and in a coordinated way, to assess the damage,
- can minimise the downtime and its impact on operations,
- the ability to restore IT services as quickly as possible.

Scope of the provision

2. §

(1) Personal scope: covers all persons who operate the University's IT or related systems, services and IT infrastructure. This shall include those areas responsible for the operation of systems to ensure the smooth running of IT services, as well as business-side experts who operate the systems.

(2) Scope: covers IT systems of high importance for the operation of the University, which store, manage, process, monitor, control and/or transmit data and information managed/owned by the University.

Concepts

3. §

(1) *IT disaster situation*: incident (IT): unexpected event. An incident is a malfunction or disruption in the use of an IT system, whether minor or major, e.g.: intrusion or attempted intrusion, data loss, data leakage, unauthorised access, virus infection, loss of availability.

(2) *IT Business Continuity Plan*: a plan to deal with unexpected events to ensure that business processes can be restored within the required timeframe.

(3) *Information technology system*: a system consisting of a combination of hardware and software used to perform various tasks of data or information processing.

(4) *Information system*: the set of processes and activities that store, produce and distribute the information necessary for the operation and management of an organisation.

(5) *Availability*: the actual state in which the availability of information or data and the operability of the system are neither temporarily nor permanently impeded.

Content of the provision

4. §

(1) The plan covers the measures to be implemented by the University's IT department.

(2) The plan does not include

- the elements that can be replaced or substituted at short notice,
- cases of IT failure that can be resolved within the 1 working day vulnerability window

(3) The IT service continuity plan only covers electronic information systems or the systems serving them, and does not address the measures and interventions required in the event of a disaster related to the provision of human resources, possible rescue or management of other assets (other than IT security services).

Related Policies, Documents

5. §

(1) The provisions of this provision shall be applied in accordance with the provisions of the IT Security Policy in force at the time.

Maintenance of the provision

6. §

(1) The plan for the continuous provision of the University's IT services in the event of an IT disaster should be reviewed regularly, on an annual basis, or on an ad hoc basis if the events listed below occur, to ensure its adequacy and effectiveness:

- when processes change,
- changes in the University's operating conditions and circumstances (physical, economic, legal, cooperation, etc.),
- when replacing critical IT tools, hardware or software that support operations.

(2) The review and maintenance is coordinated by IT.

(3) The IT service continuity plan is stored in a hard copy in a location accessible to the parties involved in its implementation, so that it is accessible at any time in the event of a corruption of the electronic version.

Testing the provision

7. §

(1) The suitability of the plan should be fully tested on a 3-year cycle. The response to the events that have occurred is also considered a test of the event and will be documented accordingly, and the lessons learned should be used.

(2) Testing is carried out as part of internal audits, in accordance with the testing plan, and documented in accordance with internal audits. If the test result is not satisfactory, the Head of IT will initiate corrective action. The action is considered closed when the test has been repeated and the effectiveness of the action is verified and the changes are recorded and finalised in the business continuity plan.

The communication route

8. §

(1) If there is a service outage that affects the entire university workforce and/or student population, the following communication process must be followed:

- The expert who detects the incident shall immediately report the outage to his/her supervisor in writing (by email), specifying the system, the reason for the outage and the exact time of the outage.
- The Head of IT must be informed immediately in writing (email) of any incident.
- The line manager (this can be any operational manager in IT) notifies Communications. The notification must include:
  - Brief description of the incident
  - Its impact, the users and systems concerned
  - The time the incident occurred and the estimated time of response
  - Proposed place of publication (intranet or website)
  - The proposed workaround (if any)
  - What to do (if applicable, e.g. power off the device, reboot, delete the specified message, etc.)
  - Person to contact in case of technical problems
- Based on these, IT and Communications staff will jointly decide on which platforms to notify staff and/or students of the service outage (intranet, website, email).

Classification of information technology systems

9. §

(1) The University's service systems are classified into four security classes according to their impact and importance. Systems that are considered critical to the service of the core business are considered to be classified as higher security.

a) Critical systems:

On the one hand, systems that are critical for the University to carry out its core activities.

On the other hand, systems that require priority protection from a data protection point of view and systems that are of high importance for the operation and/or communication of the University.

This includes:

- Central infrastructure (servers (server and hypervisor), SAN switch, storage)
- Central network devices
- DNS servers
- Central Logon Server (Active Directory)
- DB servers (Oracle)
- Student learning system and related student service systems: Neptun
- Moodle
- University website (uni-corvinus portal)

b) Featured systems:

Systems of high priority for the performance of certain important activities of the University, which are primarily technical in nature and the data stored on them are primarily non-personal.

- DHCP servers
- Radius authentication system
- Complete wired network (active and passive devices)
- KIM
- Central user management system (Cusman/AD360)
- Central computer management system (SCCM)
- M365 Sync Server (EntraID Sync)
- Central filing system, Poseidon
- Complete Administration, Service and Payroll System: SAP

c) Normal systems:

The users of systems and services that are not of high priority for the daily operation of the University as a whole are limited to certain institutions and groups of the University. They may also contain personal data that need to be protected.

- Wi-Fi network
- VPN servers
- IT support servers (License, antivirus, samba)
- Telephone exchanges (IP and traditional)
- Student computer labs
- MyCorvinus and related systems

d) Other systems:

Their operation has no impact on the University as a whole. They support the teaching, study or research work of smaller groups or individuals. This includes all other systems not included in the above categories. They may contain sensitive data that needs to be protected from incidents. They should be prioritised in terms of quantity.

- Computer workstations for teachers and researchers connected to the University network
- Printers connected to the University network
- Student free-use computer workstations

(2) In the event of failure or malfunction of Critical and Priority Systems, the communication protocol set out in this provision shall be activated and the necessary incident response measures shall be implemented.

Essential elements to ensure IT service continuity

10. §

(1) The critical infrastructure is located in the server room of the Salt House. This is where the servers and central networking equipment are located, providing access to systems that are not installed on the ground. Without the smooth operation of these, it is not possible to provide services and neither Critical nor Priority Class systems can be accessed.

Location of critical data centres:

- Data Centre 1 and 2.
  - 1093 Budapest Fővám tér 13-15., Sóház, I. floor 108
  - 1093 Budapest Közraktár utca 4., Building C, Room 14
- The point of delivery of the leased line Internet service:
  - 1093 Budapest Fővám tér 13-15., Sóház, I. floor 108
- Switchboard
  - 1093 Budapest Fővám tér 8., Building E 343

(2) **Physical security in data centres**

The entrance to the data centre is provided by an authenticated access system (card or fingerprint).
The physical security of the data centres is guaranteed by the Campus Services department in accordance with internal rules.

(3) **Uninterruptible power supply for data centres**

Parameters of the uninterruptible power sources supplying the data centre on the Main Campus 1 and 2:

- Type: Eaton 9355-30-N-0 Power: 30 kVA Data Centre 1.
  - Role: powering the data centre's uninterruptible power supply
  - Transit time: 29 minutes
- Type: APC Smart-UPS 3000 power 3 kVA Data Centre 2.
  - Role: uninterruptible power supply for rescue infrastructure
  - Transit time: 12 minutes

Uninterruptible power sources are checked 1 time per year.

(4) **Diesel aggregator feeding**

The aggregator in the basement of Building E is automatically started in the event of a power failure.

The aggregator will start feeding the uninterruptible power source to the Salt House Data Centre 1 within 1 minute after the aggregator is switched on.

Measures to be taken in the event of an incident

11. §

(1) What to do in the event of **a disaster or business continuity incident affecting data centres**:

Service continuity measures should be started immediately if:

- Physical failure of any element of the critical IT infrastructure system (servers, data storage, network backbone elements)
- Any of the critical IT operator interfaces cannot be used (device consoles, AD-based services, virtualisation).
- It is not possible to log in to the systems
- Applications are not available

(2) The initiation of business continuity measures may be initiated by the head of the relevant department exercising the authority of the employer or his/her supervisor.

(3) Actions and their sequence

"T" = time of occurrence of the disaster or critical incident

Serial number	ACTION	CONTACT	Deadline
1	Notify IT Support (preferably by phone) and the Head of IT.	Observer	T+15 minutes
2	Precisely define and escalate tasks to operational managers.	Head of IT	T+20 minutes
3	Damage assessment	Perception, IT operational managers, support staff	T+45 minutes
4	If one of the circumstances listed in paragraph 11 (1) applies, the implementation of continuity of service measures shall be ordered.	Head of IT, IT Operations Managers	Max T+ 2h
5.	Information to the Head of the CIS and the Data Protection Officer pursuant to Regulation 13/2023 ET on the Rules for Data Processing	Head of IT, IT Operations Managers	Max T+ 2h

(4) Damage assessment

Damage assessment starts, where possible, with a site visit to the affected data centre or communications hub to assess the condition of the equipment.

Where possible, the status indicators of the devices should be checked.

Where possible, attempts should be made to access the administrative interfaces of critical IT infrastructure elements and the IT services running on them.

In the case of partial failures affecting a single unit, the interrelationships and the related IT services must be analysed.

IT managers and areas to be notified per area:

In all cases, you must notify:

- Tibor Sopronyi Head of IT (tibor.sopronyi@uni-corvinus.hu) +36 30 137 9483
- Réka Kohán IT Operations Manager (reka.kohan@uni-corvinus.hu)
- IT Customer Service (ithelpdesk@uni-corvinus.hu) +36 1 482 7500

In case of data centre and critical systems failure:

- Tamás Mák IT Central Services Team Leader (tamas.mak@uni-corvinus.hu)
- Gergely Dinnyés Senior Network Operations Expert (gergely.dinnyes@uni-corvinus.hu)

Final provisions

12. §

(1) This provision shall enter into force on 1 October 2024.

(2) This provision shall be interpreted in accordance with the provisions of the IT Security Policy in force at the time.