The Business Continuity Plan (BCP) for VUOS as (Research Institute of Organic Synthesis) reflects the specifics of chemical research, testing according to Good Laboratory Practice (GLP) and custom manufacturing (ISO 9001 and GMP). The main goal is **to ensure the safety of people, protect sensitive data, minimize the impact of accidents on the environment and contractual obligations** .

- **Purpose of the document** : Ensuring the continuity of critical activities of VUOS as (research, custom manufacturing, toxicological testing) during emergencies.
- **Scope of validity** : Applies to all employees, laboratories, pilot plants and external suppliers of VUOS in the Semtín Zone area in Rybitví.
- **Frequency of revisions** : At least once a year or when there is a fundamental change in technology/legislation.

1. Business Impact Analysis (BIA) and Critical Processes

takes into account a unique mix of chemical custom manufacturing, research subject to Good Manufacturing Practice (GMP), analytical and toxicological testing (GLP), and strict environmental and safety standards in the industrial complex.

A) Impact evaluation criteria

A scale of 1 (Negligible) to 5 (Catastrophic) is used to assess the impacts of process outages in VUOS.

- **Financial** : Direct damages (spoiled batches, destruction of test cells/death of organisms), contractual penalties for failure to meet production/study deadlines.
- **Regulatory / Legal** : Loss of GLP/GMP certifications (loss of primary data), sanctions from the Czech Environmental Inspection (ČIŽP), the State Office for Nuclear Safety (SÚJB), the Fire Department, the Regional Hygiene Station, the Labor Inspectorate and others.
- **Reputational** : Loss of trust of international/domestic pharmaceutical and chemical partners.
- **Environment and OHS** : Threat to employee health, release of toxic substances into the air or wastewater.

B) Classification of VUOS processes and determination of parameters (RTO, RPO, MTPD)

The following table defines the critical VUOS processes ranked by recovery urgency.

Identifier	Key process	Financial / Reg. impact	MTPD	RTO	RPO	Critical dependencies
VUOS-01	**Reactor cooling and safety** (semi-operation/production)	5 (Catastrophic)	15 minutes	**0-15 minutes**	ON	Cooling water, inert gas, electrical energy, measurement and control
VUOS-02	**Toxicological testing / Organism breeding**	5 (Catastrophic)	2 hours	**2 hours**	ON	Ventilation, filtration, stable temperature/lighting, backup power
VUOS-03	**Data recording from analytical instruments** (HPLC, MS, NMR)	4 (High)	4 hours	**24 hours**	**0-15 minutes**	LIMS (laboratory information system), validated IT networks, data storage
VUOS-04	**Wastewater treatment and emission monitoring**	1 (Negligible)	6 hours	**4 hours**	ON	Energy, neutralization chemicals, functional sensors
VUOS-05	**Reception and storage of hazardous precursors**	2 (Low)	24 hours	**12 o'clock**	ON	Logistics, temperature control in warehouses, fire safety

VUOS-06	**Registration of chemical substances (REACH) / Consultation**	2 (Low)	5 days	**48 hours**	4 hours	ERP system, secure external access for experts, email

Explanations: ***MTPD*** *: Maximum Tolerable Downtime;* ***RTO*** *: Recovery Time Objective;* ***RPO*** *: Maximum Permissible Data Loss.*

All risks arising from the operation of VUOS, including scenarios and risk analysis, are listed in the Safety Report, Chapter 3, in accordance with the requirements of Act No. 224/2015 Coll. - Act on the Prevention of Major Accidents. It contains a risk analysis of all processes using the HAZOP method.

C) Detailed analysis of critical points

VUOS-01: Cooling, heating and reactor safety (custom production)

- **Impact of failure** : Exothermic reactions can go into an uncontrolled state without cooling (risk of explosion, fire, release of toxic gases), chemical mixtures can solidify in the reactor without heat supply, preventing the circulation of absorption media can cause emissions of hazardous gases into the environment.
- **Consequence** : Total destruction of technology, threat to life in the area, massive ecological disaster.
- **Responsibility** : According to the production line – Section 30 – Organic Research or Section 40 – Production

VUOS-02: Toxicological and ecotoxicological testing

- **Impact of failure** : Failure of air conditioning or water filtration will cause death of test organisms (fish, algae, invertebrates) or damage to artificial tissue cultures.
- **Consequence** : Devaluation of long-term, internationally certified studies. Financial losses in the order of millions of CZK, the need to repeat tests from the beginning, fatal delays for clients.
- **Responsibility** : Section 60 - CETA

VUOS-03: Laboratory Information System (LIMS) and Analytics Data

- **Impact of outage** : Inability to save validated data in GLP mode.
- **Consequence** : If data is not recorded continuously and in accordance with Data Integrity, the entire analysis is invalid. The auditor may withdraw certification.
- **Responsibility** : IT

VUOS-04: Wastewater treatment and emission monitoring

- **Impact of outage** : Inability to immediately complete wastewater treatment by stripping or neutralization. The process will terminate spontaneously. Release of substances into the air or sewer is minimal.
- **Consequence** : there will be a loss of wastewater treatment capacity and the start-up of further production will be delayed.
- **Responsibility** : Section 40 - Production

VUOS-05: Reception and storage of hazardous precursors/thermounstable substances

- **Impact of outage** : Inability to control storage conditions, inability to receive and issue chemicals.
- **Consequence** : Threat to the quality of stored substances, financial loss.
- **Responsibility** : Section 50 – Trade and Logistics

VUOS-0 6: Registration of chemical substances (REACH) / Consultation

Impact of outage : Inability to provide services to the company and external customers

- **Consequence** : Financial loss
- **Responsibility** : Section 60 - CETA

Specific dependencies and gaps

- **Human resources** : VUOS processes require highly specialized personnel (chemists, toxicologists). The absence of key personnel (e.g. pandemic, mass poisoning) paralyzes laboratories.
  Substitution is addressed by the directive According to the directives LOS 00 01 – Organizational Rules and POS 00 14 – Transfer of Functions. It is also part of the Safety Report, Part 5 according to Act No. 224/2015 Coll.
-
- **Critical infrastructure** : Strong dependence on the continuity of energy and media supplies (nitrogen, steam) within the Semtín/Pardubice industrial area. Service Level Agreements (SLAs) with energy providers correspond to the specified RTOs. The primary supplier is Synthesia Power as, the secondary supplier is ČEZ Distribution.

2. Crisis organizational structure and communication plan

The crisis organizational structure and communication plan are described in detail in the VUOS Emergency Plan, which is an annex to the safety report in accordance with the requirements of Act No. 224/2015 Coll. Further details on safety and threat levels are provided in the Physical Protection Plan and Directive POS 0066 - Measures in the event of a security threat to VUOS as

VUOS customers are informed about force majeure and product supply outages or delays in certified studies - see Appendix 1.

3. Strategic scenarios of crisis events

Examples of scenarios from different areas of activity"

Scenario A: Infrastructure Failure (Blackout / Cooling Failure)

- Immediate actions: Automatic activation of UPS for instruments and MaR, start-up of diesel generators for reactor cooling and ventilation of the breeding of test organisms.
- Critical limits: If power is not restored within 2 hours, a safe, controlled shutdown of running chemical reactions occurs according to technological regulations.

Specific scenarios for each VUOS space are included in the Security Report, Part 3.

Scenario B: Cyber Attack (Ransomware / IT Outage)

- Immediate actions: Isolate affected network segments. Since key computers are not connected to the network, this only affects regular office computers.
- Data integrity: not compromised, data is stored on two independent servers and can be restored within a maximum of 24 hours.

Scenario C: Ecological accident / Leak of hazardous substances

- Immediate actions: Evacuation of affected buildings, activation of emergency sumps, closing of sewer valves in the area.
- Coordination: Immediate notification of the company's Fire Rescue Department and the dispatch center of the Synthesia parent site.

  Specific scenarios are based on Act No. 167/2008 Coll. - Act on the Prevention and Remediation of Environmental Damage under the title Detailed Assessment of the Risk of Environmental Damage. Further description is part of the LOS 00 10 Directive - Water Management Emergency Plan VUOS and the Integrated IPPC Permit.

2. Recovery and continuity strategy

Production and laboratories

- **Backup power supply** : VUOS has **2** diesel generators that automatically start up in the event of an interruption in the electricity supply. These backup sources cover the entire production capacity of buildings Ry 11, Ry 13 and Ry 114. Furthermore, the operation of toxicology laboratories on Ry 114 and the cooling and monitoring systems of warehouses Ry 114.
- **Supply crisis** : Alternative suppliers of strategic chemicals are contractually secured. VUOS always has at least two independent sources of raw materials for critical raw materials. Access of suppliers to the company is governed by the External Emergency Plan and the specific level of threat. Which are described in the guidelines POS 42 - Entry of persons and vehicles into VUOS and POS 00 66 - Measures in case of threat to the security of VUOS as

IT and data management

- **Geographic backup** : Laboratory data and research results are replicated to a secondary location (remote data center). The primary is building Ry114, the secondary is building RY 12.
- **Access protection** : Strict segmentation of the operational network (production control, analytical measurements, etc.) from the corporate network.

- **Power supply** : Key computers have UPS backup power sources. In addition to 6-hour backup power sources, the servers are connected to a diesel generator that starts up 5 minutes after a power outage.

  A detailed description of the operation of the VUOS data network, backups, and user rights are described in Directive POS 00 61.

6. Testing, maintenance and updating the plan

- **Quarterly tabletop exercise** : Simulation of crisis scenarios (e.g. ransomware) at management level – twice a year, a thematic exercise is held according to the directive POS 00 63 - Basic crisis situation training. The directive specifies which situations the exercise should cover
- **Annual technical tests** : Real tests of switching to backup energy sources and restoration of critical IT systems from backups – backup sources are tested every 14 days for 20 min. according to the Air Protection Act No. 201/2012 Coll. and as part of the operability check according to Decree No. 246/2001 Coll. – Fire Safety Decree
- **Compliance audit** : Update the plan whenever legislation changes or when purchasing new significant laboratory technology – all guidelines are updated according to VSQ 05 00.