BUSINESS CONTINUITY PLAN

18th August 2021

Granite company level

1. Overview

Granite's business continuity plan describes how to maintain corporate business continuity in the event of a business disruption. The main purpose is Granite's continuous operability and smooth, functional, reliable, secure and available services to all customers.

Guaranteeing the smooth course of business operations and the customers' trust in Granite's ability to deliver the agreed-upon services is the key element for us.

This business continuity plan outlines the aims and means how to make sure customers face minimum harm in the case of disruption or any other incident affecting to Granite's businesses.

Granite's offering and operations are built on modern platforms so there are only a limited number of situations, which could stop the service production. Granite's solution is typically not one of the most availability critical for customers so from that perspective short service downtime will not normally cause any major harm.

2. Definitions

Business continuity failure means that Granite is not able to either partially or fully operate and deliver services to customers. In each customer agreement is defined response times and service level. These definitions are based on Granite's business culture and Service Level Agreements (SLA) made with service providers and subcontractors.

Main business continuity threats to Granite are:

- IT failure
- Network failure
- Information security incidents
- Electricity cut down
- Several key persons unable to work
- Office cannot be reached

3. Scope and objectives

This business continuity plan concerns all of Granite's operations, i.e. all the different areas of business and services. This plan is observed in terms of applicable parts between Granite and its service providers and subcontractors.

The aim is to make Granite prepared if any business continuity issues are about to rise. This business continuity plan forms the basis for this issue and together with Granite's Information Security Policy and Information Security And Privacy Description they form the body how Granite is prepared on possible disruptions facing the company.

Recovery time objective (RTO) is two days in case of major disruption or disaster. Recovery point objective (RPO) is one day.

In addition, the aim is to achieve the level of business continuity readiness, which meets industry standards and the requirements of the customers.

4. Organization and responsibilities

Granite's CEO is the highest party making decisions on business continuity issues. The CEO will approve the business continuity plan and the amendments made to it. Plan is reviewed annually by CEO and reported to the Board of Directors.

The CEO is responsible for coordinating business continuity and may allocate responsibility for parts of the whole to other members of Granite personnel. The Security Team described in the Risk Management Policy is responsible for processing deviations related to business continuity and the necessary procedures. There will be always at least two persons processing and investigating deviations.

Each employee is responsible for business continuity for their own part by operating in accordance with the training and guidelines provided. Each employee is responsible for reporting problems and deviations related to business continuity to the CEO or Security Team.

5. Implementation methods and principles

IT failure

- Server hosting service is out of business
    - Granite has agreements with two separate server hosting/data center service providers, which can take over if the other is out of service.
    - Centers are located in different physical locations, which also mean totally separate power supply, data connection networks, etc.
- Server problems and breakage
    - Virtualized and doubled environments secure service availability in server break situations.
    - Server level disaster recovery is tested annually by Granite in co-operation with the datacenter Service Provider(s).
- Database corruption
    - Active database backup and restore procedures are tested and verified annually.

Network failure

- Long lasting operator/ data connection problems
    - Granite solution offering is based on internet connection. With servers running, nothing else is needed. There are normally several suppliers offering network connections so in case of one operator is out of business other options are available.
    - Granite's data center service providers have multiple operator connections in their data centers, so they are not dependent on one operator.
    - All Granite's employees have possibility to work remotely with necessary equipment.

Information security incidents

- All Granite employees have guidelines how to act if they detect or suspect any kind of information security incident.
- Person who detects an incident will document the incident to incident management system and inform Granite's Security Team immediately. Security Team has responsibility on coordinating necessary actions.
- Granite has an information security insurance that provides professional services for incident response and investigation. This insurance will be utilized in the event of information security incident.
- After every incident, the need to update guidelines and policies is assessed based on risk assessment of the incident.
- There is a possibility to cut down access to service if there's a strong suspicion that the service is compromised and there's a possible data breach.
- Service providers offering server hosting and data center services to Granite have information security solutions in place to continuously monitor in- and out-going data traffic in their center. In the case of intrusion or attack they'll inform their customers immediately and start necessary actions. Granite acts accordingly towards own customers and starts own investigations and possible corrective actions.
- The National Cyber Security Centre Finland (NCSC-FI) will be informed by the Security Team and based on NCSC-FI instructions and recommendations additional actions shall be taken. NCSC-FI helps organizations to fight cyber-crime.

Electricity cut down

- In Finland and especially in major Finnish cities electricity network is almost 100% reliable and built in circles so that breakages and faulty components can be bypassed. Data centers have reserve power generators and UPSs to manage power cuts.
- All Granite's employees have possibility to work remotely with necessary equipment, working is not place dependent.

Key persons unable to work

- Competencies and capabilities in Granite are spread so that all roles and tasks can be operated by more than one person.
- With continuous training and personnel development will be made sure that organization stays all the time operational from competence perspective.

Office cannot be reached

- All Granite's employees have possibility to work remotely with necessary equipment, working is not place dependent.
- If temporary office premises are needed both in Tampere and Helsinki areas there are operators who rent short-term office space. Moving office to another location takes one to two days.
- Premises owners/landlords arrange emergency exercises on a regular basis according to Rescue Department authorities' instructions and Granite takes part on them as obliged.

Reporting

- Any case related to business continuity which have implications to any customer, customer will be kept informed and necessary reports requested by each customer will be provided to them.
- In major disasters the social media and other channels are utilized to get information to as many users as possible.
- Granite board will be kept informed by CEO about continuity break status and corrective actions.