Welocalize Disaster Recovery & Business Continuity

Introduction

This policy is Welocalize business continuity program for the organization's infrastructure and services. Any additional business continuity management for other products and services are designed and built around this policy.

The business continuity policy includes references and high-level information on the organization's business critical cloud service provides and how these providers manage disaster & business continuity.

It also covers the disaster recovery of the systems hosted in Welocalize managed colocation facilities.

Information Security and Information Technology contact list, Emergency Management contact list and a list of contacts for the critical systems/services.

Policy

Definition of disaster

Any malicious cyber-attack that may result in loss of services (such as a DDoS attack), a pandemic which may result in loss/unavailability of human resources or any catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Welocalize operations.

What we do

Information Security continuity is integrated into the cloud systems utilized within our organization and are designed to survive any type of disruptive event.

Information security continuity is designed based on the probability of occurrence considering the confidentiality, integrity and availability of the information and assets on the business' ability to continue performing as expected.

As part of the broader risk assessment, events that can cause interruptions to business processes are identified, along with the probability and impact of such interruptions and their consequences for information security. This is already conducted in our documented information security risk assessment process and our Risks and Treatment Plan.

For our hosted services

Some of the Business Continuity and Cybersecurity components of our hosted services include:

- Incorporation of encryption-at-rest, in process, and in transit for all information assets.
- 99.9999% uptime for our asset storage infrastructure meaning less than 32 seconds of downtime a year.

- Hosted solution provides for ease of connection and flexibility of location in the case of physical power or facility outages all uploads, downloads and file activities are time and date stamped with the user ID for forensic evidence trails.
- Flexible user ID parameters allow us to set strict permissions down to the folder and file level to enable enforcement of “least privilege”.
- Limited life links ensuring that access to data for translation is only available during the active project phase unless worked in a closed system.
- Files are stored inside AWS S3 storage, which does near real-time replication of data into three different physical locations. Thus, if two geographically diverse areas are down, a third is still up and running and provides secure access to the files.
- Near real - time replication with versioning removes traditional backup requirements and allows us to immediately restore files to previous versions.

For our colocation hosted services

We conduct regular backups of systems hosted in Welocalize managed colocation facilities using industry standard backup software and tools.

Our backup plans are documented and maintained in our documentation system. The backup plan includes daily, weekly or application aware backup procedures as well as retention strategies for each procedure.

Our Disaster Recovery plans are also documented and maintained in our documentation system. As part of our disaster recovery for hosted services we utilize Microsoft’s Azure Site Recovery which allows us to restore any system and its functionality/accessibility in a relatively short period of time.

Access to ISMS documentation in the case of an event

All our ISMS documentation is stored and maintained in our SharePoint and our Confluence cloud to help mitigate any issues about the ability to access the ISMS during an event as the services are 'always on' and hosted in the cloud. The plan is accessible to authorized users from any location there is internet access.

Testing

Backup validation

Backups are validated at least once per year to ensure backup processes are working as expected. A more constant testing takes place as part of our everyday operations requirements, as users frequently request restoration of data for various purposes.

The backup validation process is documented and maintained within our documentation system.

Disaster recovery

For disaster recovery we are validating Site Recovery at least once per year. The site recovery process is documented and maintained within our documentation system.

Disaster recovery plan

Identification of disaster

Welocalize is a global organization which operates on a 24/7 basis. To be able to identify a disaster, the organization has deployed a state-of-the-art SIEM (Security information & Event Management) system which is configured to notify our global Information Technology team in case of a cyber disaster occurring.

In case of a non cyber disaster (such as a pandemic) the organization's global management is notified to assess the situation and decide on a course of action.

In case of a catastrophic event, local management and emergency teams are notified to assess the situation and decide on a course of action.

In the event of a Catastrophic disaster

In the event a catastrophic disaster occurs in any of the organization's offices around the world, local management, and emergency teams, with the help of local authorities as applicable, assess damage, consult with vendors/providers of equipment to ensure that their expert opinion regarding the condition of the equipment is determined ASAP.

Affected equipment may include communication, Internet equipment, office furniture and other office space.

If the affected facility is accessible, conduct an on-site inspection of affected areas to assess damage. Gather recommendations for required resources.

Operations recovery

Welocalize is not hosting any operations related infrastructure in offices. All employees are equipped and able to remote work from any location where Internet is available. Thus, recovering operations in specific location is not considered to be a problem.

In all other cases, operations is not disrupted by a disaster.

Annex I: Contact Information

Cloud service provider

For each of our service providers we have accounts and access to their support ticketing systems as well as a dedicated contact in case of emergency.

Information Technology & Security team

Welocalize emergency team for responding to cyber disaster is consisted of the following roles:

- Vice President of Global IT
- Head of IT Engineering, Global IT
- Head of IT Support, Global IT
- Information Security Manager

Our global support team can be reached via our official ticketing system on a 24/7/365 basis.

Emergency teams

For each location a local emergency team is formed, and contact information is shared among the members.

Local emergency services like fire brigade, police or medical emergency services are included in that contact information.

Where applicable, a company doctor and a safety officer are appointed, and their contact information shared with the local emergency team.

Local emergency teams and their contact information are documented and maintained in our documentation system with access to authorized personnel.