June 1st, 2020

Business Continuity Policy

Business Continuity Policy sets up the framework to:

- protect our people, systems and infrastructure
- identify and mitigate the risks to our operations to an acceptable level
- manage any disruption to minimise its impact
- ensure our customers receives our services as per SLA

Responsibility

Mondeca's CEO and COO are responsible for ensuring that the business continuity policy is defined, updated and implemented. The entire staff has a responsibility to ensure that the aims of the policy are met in their areas of activity.

Policy aims

We endeavor to:

- Identify risks
- Set up organizational and technological approaches to minimize their impact.
- Continually improve and monitor our approach to business continuity.
- Incorporate business continuity factors into business decisions.
- Increase employee awareness and training.

People

- The safety of people is our primary concern. We react as quickly as we can to all safety related issues. For the Covid-19, we organized the company as a virtual team several weeks before the government ordered lockdown.

Infrastructure

- Ownership and management of systems and networks infrastructure is not within Mondeca's core competencies. We do not own nor do we have on our premises any significant hardware components. Our infrastructure is located with world class providers - AWS and OVH. We monitor our suppliers business continuity plan and organize our infrastructure to take advantage of it (ex through facilitating the delivery of our services from different AWS regions and/or infrastructure vendors).

Offices

We minimize/remove risks related to our premises.

- We do not have any infrastructure components located on our premises.
- Headquarters are not an access point for our network, nor a hub for data exchanges.
- We do not store any data at our offices.
- Our telephone, videoconferencing and messaging facilities are not hosted at our offices.
- Our organization can operate as a virtual team without any impact on services.

Our policy is to entirely remove risks related to office availability.

Suppliers and subcontractors

- Dual supplier policy is implemented for business critical supplies and subcontracting.

Cybersecurity

We minimize the risk of cyber attacks through:

- Regular back ups of systems and data
- Monitoring and reporting all security incidents
- A "share nothing" approach for customer systems, to avoid impact of a potential security breach of one client system on other customers.

Monitoring and improvement

- We comply with and exceed all relevant regulatory requirements.
- We continually improve and monitor our approach to business continuity
- We review this policy and any related issues at our monthly management meetings.

Culture

- We involve staff in the implementation of this policy.
- We update this policy at least once annually in consultation with staff