January 12, 2021

Cyber Security Policy

Responsibility

Mondeca’s CEO and COO are responsible for ensuring that the cybersecurity 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:

- Ensure that information we manage on behalf of our clients is secure.
- Ensure that applications we deliver to our clients are secure and operate without disruptions.
- Ensure that we can support our clients without disruptions.
- Increase employee awareness and training.

Infrastructure protection

Our guiding principle of infrastructure protection is to have our infrastructure managed by vendors having the capacity, expertise and excellent track record in cyber security. Our primary suppliers are Amazon Web Services and OVH.

Physical and environmental security

Mondeca does not own nor have on it’s premises any critical infrastructure components, except employees workstations and local network area equipment. All key components, without exceptions, are located in secure data centers of either AWS or OVH.

Employee network access

- Remote access to the company network is accessed through secure VPN only.

January 12, 2021

Password policy

- Use of secure, system generated passwords is required whenever possible.
- Passwords lifetime may not exceed 60 days.
- Usage of accounts on various systems is periodically reviewed. Unused accounts are removed.

Incident handling

- Security incidents must be immediately brought to management attention.
- All security incidents require a written report, including incident description, identification of actual and potential consequences, root cause analysis, short term remedials and structural changes implemented to avoid similar incidents in the future.
- If the incident involves client systems or data, information, including the final report, is shared with the client.
- Incidents involving personal data loss must be reported to authorities according to European data protection and data privacy laws and regulations.

Monitoring and improvement

- We review this policy and any related issues at our monthly management meetings.

Client data

- Use of client data for testing purposes is not permitted without client authorization.

Culture

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