IT Security Policy

This document is a description of how Wasabi Web handles IT-security for internal and external use.

Servers

Network / Internet / Geographic / Infrastructure

We use three co-locations

- Bahnhof S:t Erik (Stockholm) - Primary location with three incoming fibers and one fiber between Leica.
- Bahnhof Leica (Stockholm) - Secondary location in a military-graded steel building which serves as a recovery and backup location. Will go online if S:t Erik is offline.
- Östhammar - Third location in a concrete bunker which serves as a recovery and backup location. Will go online if Primary and Secondary is down.

Locations have redundancy for everything (network card, switches, firewalls etc).

Power

Battery powered (UPS) in case electricity goes out, which will keep the servers live until the diesel generator is running.

Environmental

Renewable energy and eco-labeled with the certificate Triple Green.

Physical security

- Multiple security systems to enter building
- Physical locks at server racks
- Camera Surveillance 24/7/365
- Personal at location - Day time
- Surveillance by Security Company - Night time

Web security

- WAF: Web Application Firewall
- Atomic Secure Linux Full Modsecurity Rule Set
- SQL injection protection
- Denial of Service protection

- Brute force protection
- Virtual patching of Applications
- Protection within Wordpress
    - Local Brute Force
    - Network Brute Force
    - Automatic Lockouts
    - Password enforcement (strong passwords)
- 2 Factor Login before Wordpress login
- Fail2Ban

Data within Wasabi Web

All employees at Wasabi Web AB have signed an employee contract where client information stays within the company and is not exposed for third parties.

Data outside EU

See attached links for further information about systems we use https://wasabiweb.se/gdpr/.