General Security Measures

While more technical details are reserved for preserving the integrity of the security systems in place, here are some of the most relevant safeguards applied:

Server and Infrastructure Protection

- 24/7 server monitoring
- Server and infrastructure security configuration consistently applied across all servers
- Firewall protection
- Advanced security modules that assure the best possible protection, such as mod_security, Suhosin PHP hardening, PHP open_basedir protection, and others
- Anti-malware protection on endpoints and servers

Procedures and Practices

- A dedicated internal Security team Implemented internal policies and procedures to support information security
- Continuous scan for vulnerabilities and penetration testing
- Responsible Disclosure Policy Applied OWASP secure coding practices and other industry standards
- 2FA authentication enabled on all applicable systems

Data Integrity

- All operating systems are kept up to date, including security patches
- Database encryption with secure hashing algorithms
- Regular data backups
- Continuous static code analysis to detect potential code security issues