Exware Cyber Security Features & Policies

Physical Security

The servers are kept in a locked cage in a datacentre, which is protected by a mantrap with two locked doors requiring passkeys, a passcode, and a fingerprint scan.

The building is locked outside of business hours and has 24/7 on-site security.

Server Security

No shell-level access to server, except by Exware staff, who can connect through encrypted sessions (ssh) only.

The only Internet services that can connect to shared hosting webservers are Web (http, https), Email (POP, SMTP), Domain Name Service (DNS), and Secure Shell (ssh). All other services are disallowed, including FTP. Some webservers operate with fewer services. Private servers configuration can be customized to client needs, but by default would only have Web (http and optionally https) and Secure Shell (ssh).

SSL (https) is supported for secure websites. A generic secure website (secure.binarylock.com) is available for websites that do not have their own SSL certificates.

No PHP or untrusted 3rd-party applications are permitted on the webserver.

The servers are standardised on Ubuntu Linux LTS, and are protected by a Firewall as well as an intrusion prevention system.

Our servers are monitored 24/7 from three independent monitoring stations, with real-time alerts for Exware staff.

Servers are backed up daily. Backups are stored off site to two locations. Website owners can obtain copies of their own backups through the web administration panel.

Database Security

The database server is accessible only on a private LAN subnet, not accessible from the Internet.

Web applications can only see their own private databases, not those of other sites.

No direct access to database, except by Exware staff.

Database access tools have additional security layers to control access to individual tables, rows, and columns.

Application Security

No sensitive financial data such as credit card numbers are handled or stored by your web applications. All credit-card processing is outsourced to 3rd-party payment gateways.

Multiple levels of administrator access for web-based site management.

Multiple CMS roles to partition content management duties.

Websites can be broken into sections for better partitioning of duties.

Moderation functions (administrator approval of user-generated content) available for many web applications.

Applications will automatically screen data from view if the user is not permitted to view it.

Many applications will generate e-mail notifications of significant updates to your data.

User Security

Users can be granted login access to specific sections, to view member-only pages or functions.

Features such as password reminders, persistent logins, user-changeable passwords, and user-changeable name/email, are all configurable to suit each site’s security rules.

Password storage is normally done through a 1-way encrypted hash function. Less secure storage schemes can also be supported, although these are not recommended.

System supports customizable password validation (e.g. testing that passwords conform to local rules for password strength).

System supports customizable authentication procedures, including external authentication services.

Privacy and Use of Data

Exware hosts client data on its servers for the purpose of running client websites. Copies of the data are made for backups, and in some cases for purposes of testing and software development.

This data includes website content, member and user information, plus any other information, documents, and files collected by the website and/or added by the client through various means, including data imports and uploads. This data is not shared, sold, or redistributed to 3rd parties in any form, except where specifically authorized by the client. Each client retains ownership of their data and Exware makes no intellection property clames on client data.