



Data Security

YOUR USE OF THE PLAYERXP (TOGETHER WITH ITS AFFILIATES, "PLAYER XP REPORT", "HERTZIAN API" OR "US"/

"WE"/ "OUR") WEBSITES (THE "SITES"), MOBILE APPLICATIONS AND ANY SERVICES OFFERED BY HERTZIAN'S

NETWORK OF PROPERTIES (COLLECTIVELY WITH THE FOREGOING, THE "SERVICES") IS SUBJECT TO YOU AGREEING TO THESE TERMS AND CONDITIONS (THESE "TERMS"). IF YOU DO NOT AGREE TO

THESE TERMS, THEN YOU MAY NOT USE THE SERVICES.

Data Security

We're in the business of data analytics, so the privacy and security of that data is just as important for us as the products we create using that data. We continually invest in maintaining security standards whilst making sure we protect the confidentiality of our users' and data. We take a comprehensive approach to data security, which is outlined below.

Encryption for Sensitive Data

Sensitive information you exchange with Player XP is always encrypted in transit. Any time you enter a password on the Player XP website, look at any of your data, information will be transmitted using the SLL encryption protocol.

You can check this by looking for the "lock icon" in your browser's address bar.

SLL encryption is the industry-leading standard for transmitting private information, such as usernames, passwords and banking information, over the Internet.

Hosted on AWS Secure Servers

Your information is stored securely. Your username and password, including any of those of 3rd party services you have linked with Player XP, and are always stored in encrypted format.

The IT infrastructure that AWS provides to its customers is designed and managed in alignment with best security practices and a variety of IT security standards. The following is a partial list of assurance programs with which AWS complies:

1. SOC 1/ISAE 3402, SOC 2, SOC 3
2. FISMA, DIACAP, and FedRAMP
3. PCI DSS Level 1
4. ISO 9001, ISO 27001, ISO 27017, ISO 27018

Security Tested Regularly

We monitor the security of our hardware and software on a regular basis. Our services are reviewed, monitored and tested regularly by the team.

We use firewalls to protect our internet connection. This will be your first line of defence against an intrusion from the internet.

We choose the most appropriate secure settings for our devices and software Most hardware and software will need some level of set-up and configuration in order to provide effective protection.

We control who has access to your data and services. Restrict access to your system to users and sources you trust.

We protect ourselves from viruses and other malware. Anti-virus products can regularly scan your network to prevent or detect threats.

We keep our software and devices up-to-date. Hardware and software needs regular updates to fix bugs and security vulnerabilities.

We regularly backup our data. Regular backups of your most important data will ensure it can be quickly restored in the event of disaster or ransomware infection.