



JHP 014S DATA SECURITY STATEMENT

February 2024

At JHA, ensuring the security and privacy of our customers' data is our top priority. Our approach to risk management includes the following measures:

Asset Management:

We maintain a centralized database for recording IT assets, with designated business owners for each asset. Information is classified and securely stored, with backups stored in different locations and regularly tested.

Physical Security:

Our office facilities are equipped with standard security measures, including alarms, CCTV, and electronic access control. Access to information processing facilities is restricted from public areas.

Network Security and Patch Management:

Our network security includes firewalls, zoning, and regular penetration tests by third parties. Patch management processes ensure timely execution of security patches, with regular testing to address vulnerabilities.

Access Control:

Access to sensitive data is regulated on a "need-to-know" basis. We conduct regular reviews of access rights and maintain comprehensive logs to ensure accountability and traceability.

Business Continuity and Disaster Recovery:

Our business continuity and disaster recovery plans integrate security and risk requirements. Through frequent reviews and updates, we ensure that critical systems and data are backed up and tested for reliability. Swift restoration measures are in place to minimize downtime during an unforeseen disruption. In the event of a data breach, we have outlined immediate response protocols and containment measures to minimize any potential impact on your data.

At JHA, we are committed to maintaining the security and privacy of your data. If you have any questions or need further information, please feel free to reach out to us.