

Bankhawk IT Security Policy

Risk Management Procedure

Potential hazards to data and systems are continuously monitored:

- Physical threats – office fire, power failure, malicious damage, theft.
- Human error – input error, mistaken processing of data, careless disposal of data.
- Threats from corporate espionage, malicious damage, malware and viruses.

The security of data and information systems is monitored on an ongoing basis in order to identify specific areas of vulnerability and to provide appropriate safeguards against same. Bankhawk controls:

- Who has access to what information
- Who uses the data and how they use it
- Whether access is restricted to those who need data for their work
- How passwords are used and updated
- What anti-virus software and firewalls are in place to protect systems
- Levels of staff training and supervision

With this level of control in place, data and systems that are most critical can be assigned additional security safeguards.

IT Security Policy

Bankhawk's IT security policy covers both external threats (viruses, etc.) and internal threats (data theft, etc.) and is used by management and employees to ensure every reasonable effort is made to protect all data within the power, possession and control of the Company. In particular the IT security policy includes:

- Secure login identification for using IT systems
- Logical access controls – limiting employee access to information and restricting access to the level needed for each job
- Security of client data
- Plans for business continuity management

Server and Data Storage

Bankhawk recognize that data security is absolutely essential when dealing with confidential information belonging to clients. Bankhawk have put comprehensive security measures in place and use the latest in server technology to ensure that all client data is maintained in a secure environment. In particular Bankhawk have addressed the following key issues:

- Physical security – Bankhawk servers are kept under lock and key in a secure environment with 24 hour supervised security.
- Access privileges – only senior IT management are granted access to servers and must get clearance from senior management before doing so.
- Firewall – Bankhawk use the latest in firewall technology to monitor what goes in and out of systems and to block anything that may be a threat according to a predefined, rigorous set of rules.
- Encryption – all client data stored on Bankhawk servers is encrypted using the very latest encryption software.
- Physical back up – all client data is backed up periodically onto specific Bankhawk storage devices which are kept under lock and key by management only.

Viruses

Bankhawk employ the following procedures for dealing with viruses:

- Commercial Anti-virus software is installed to detect viruses, stop them running, delete them and repair any damage caused. Bankhawk uses Symantec Endpoint Protection, the next generation of AntiVirus with unmatched defense against threats for laptops, desktops, and servers.
- Security functions are used to restrict surfing on specific high-risk websites. Bankhawk uses SonicWALL Internet Security Solutions which includes devices that provide a firewall, UTM (Unified Threat Management), VPN (Virtual Private Network), backup and recovery, along with anti-spam / email and content filtering.
- Guidelines detailing acceptable use of business systems /emails follow industry norms and all employees agree to comply with same in writing.

Computer Misuse and Hacking

Hacking threats can come from both inside and outside a business. As Bankhawk Systems connect to the Internet, special precautions against 'hacking' are taken:

- Firewall – this checks what goes in and out of Bankhawk's systems and blocks anything that may be a threat according to a predefined set of rules. Bankhawk uses the Network Monitor module of SonicWALL Internet Security Solutions as firewall protection.
- Intrusion detection systems – these look for any signs of attempted hacking on the Bankhawk System and send warning alerts if such an attempt is observed. Bankhawk uses the UTM (Unified Threat Management) module of SonicWALL Internet Security Solutions to monitor for signs of attempted intrusion.
- The very latest software is used and is regularly updated as hackers generally try to take advantage of older software that contains known weaknesses. Bankhawk uses Windows XP Service Pack 3 auto-update.
- All client data is encrypted using the latest encryption software. Bankhawk uses Symantec Endpoint Encryption, which is a centrally managed software-based that enables the automated encryption of data on endpoint machines.

Internet and Email Use

Bankhawk recognises that the inappropriate use of email and the internet can lead to significant consequences for its business. To avoid inappropriate usage, Bankhawk requests that all employees sign documentation to confirm that they understand the company's strict email and internet usage policy.

Data Backup and Disaster Recovery

Bankhawk is aware that the extensive use of computer systems makes business operations vulnerable to major problems and that storage systems can be at risk to theft or physical damage through fire/flood. Bankhawk have a comprehensive back-up routine that is carried out on a daily basis and includes:

- Scheduling online backups to be automatically carried out twice daily. Bankhawk are using a specific data service provider (Datahaven) to provide this backup service. With this service provider a dedicated account manager guarantees

service levels with full monitoring 24/7 and full automation of all backups.

Scheduled backups cover all operating systems, databases as well as e-mails.

- Assigning the main responsibility for monitoring backups to the IT manager with the Operations Director covering any absences
- Ensuring that backed up information is secure and kept offsite
- Periodically testing backups to ensure that data can be successfully restored.

Disaster recovery provides cover for really serious incidents. Bankhawk have business continuity plans to determine in advance how business can survive and recover from such an incident.

Staff Training and Data Security Awareness

Bankhawk continuously communicates security policies and procedures to employees and ensures that it receives their commitment in adopting such methods:

- Staff are trained to use systems correctly and backup responsibility is assigned
- Data security procedures and principles are regularly communicated
- How particular tasks will be carried out manually if technology breaks down is planned
- IT protocols, including use of email, software and the internet as well as use of passwords is clearly set out for employees
- Staff are involved in risk assessment and in regular reviews of procedures