

ABC INTERACTIVE

Information Security Policy

Objectives

The objectives of this policy are to safeguard the Integrity, Confidentiality and Availability of all the Information handled by ABC INTERACTIVE, by making sure that:

- The Information Security Policy provides clear direction for the information security program;
- The Information Security Policy shows that management is committed to information security;
- Management supports the organization's information security policy;
- The Information Security Policy shows that management is prepared to support an on-going commitment to information security;
- The Information Security Policy is consistent with the business objectives;
- The Information Security Policy meets the organization's business requirements;
- The Information Security Policy complies with all relevant laws and regulations.

Responsibilities

The Information Systems Manager has been entrusted with direct responsibility for maintaining this policy and providing advice on information security and guidance on its implementation.

All employees have a responsibility to conduct themselves in an ethical manner. In particular:

- Data/information obtained inappropriately should not be used;
- Finding a system weakness should be reported immediately and should not be taken advantage of;
- Every user has a responsibility to carry out his/her work diligently and will be held accountable for misuse of the company's information system;
- When the confidentiality of information is unclear, its classification should be ascertained; and
- Report any known violation or system weakness to the person or persons responsible for security.

Policy

Data Classification

All ABC INTERACTIVE data must be broken into the following three sensitivity classifications:

- Public
- Classified
- Confidential

Distinct handling, labeling, and review procedures must be established for each classification.

Public: Information is not confidential and can be made public without any implications for ABC INTERACTIVE.

Classified: Information is restricted to management approved internal access and protected from external access. These are information assets for which there are legal requirements for preventing disclosure or financial penalties for disclosure. Payroll, personnel and financial information are also in this class because of privacy requirements.

Confidential: Access to this information is very restricted within ABC INTERACTIVE. The highest possible levels of integrity, confidentiality, and restricted availability are vital. It is the data owner's responsibility to implement the necessary security requirements.

Before any computer storage media is sent to a vendor for trade-in, servicing, or disposal, all ABC INTERACTIVE sensitive information must be destroyed or concealed according to methods approved by the Information Security department.

Any documents sent to the regulator or any other third party must be properly marked with the appropriate data classification.

Any Classified and Confidential documents should be stored in a safe place, or in a cabinet which is locked and only accessible to authorized people.

Downloading of Data

Electronic Mass Data Transfers: Downloading and uploading Classified and Confidential Information between systems must be strictly controlled.

Other Electronic Data Transfers and Printing: Classified and Confidential Information must be stored in a manner inaccessible to unauthorized individuals. Classified information must not be downloaded, copied or printed indiscriminately or left unattended and open to compromise.

Logon and Logoff Process

All users must be positively identified prior to being able to use any ABC INTERACTIVE multi-user computer or communications system resources.

In case a user forgets to lock their computer, if there has been no activity on a computer terminal, workstation, or personal computer for a certain period of time, the system must automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided a valid password. An exception to this policy will be made in those cases where the immediate area surrounding a system is physically secured by locked doors, secured-room badge readers, or similar technology. All other users have to lock their computer whenever they leave their desk.

Computer Viruses, Worms, and Trojan Horses

Approved and current virus-screening software must be enabled on all ABC INTERACTIVE computer systems and servers. This software must be used to scan all software coming from third parties or other departments and must take place before the new software is executed. Users must not bypass scanning processes that could stop the transmission of computer viruses.

The willful introduction of computer viruses or disruptive/destructive programs into the ABC INTERACTIVE environment is prohibited, and violators may be subject to prosecution.

The Information systems department is responsible for eradicating viruses from all personal computer systems. As soon as a virus is detected, the involved user must immediately follow the 'Incident Response Policy' to assure that no further infection takes place and that any experts needed to eradicate the virus are promptly engaged.

ABC INTERACTIVE computers and networks must not run software that comes from sources other than business partners, knowledgeable and trusted user groups, well-known systems security authorities, computer or network vendors, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from un-trusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by the Information Security manager.

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Intrusion Detection

Intrusion detection is implemented on all servers and workstations containing data labeled as Classified or Confidential.

Logon attempts to connect with ABC INTERACTIVE information systems must be logged. Operating system and application software must also have logging enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems should be enabled.

These logs will be checked on a regular basis; server, firewall, and critical system logs reviewed frequently, automated review enabling and alerts should be transmitted to the administrator when a serious security intrusion is detected.

Whenever a system is suspected of compromise, the involved computer must be immediately removed from all networks, and procedures followed to ensure that the system is free of compromise before reconnecting it to the network.

After either a suspected or demonstrated intrusion to a ABC INTERACTIVE computer system, the System Administrator must immediately notify the system's users that an intrusion is believed to have taken place, and that the status of all passwords on that system must immediately be changed to expired, so that these passwords will be changed at next log on.

Encryption

When ABC INTERACTIVE information is transmitted over any communication network, it must be sent in encrypted form. Whenever information is stored or transported in computer-readable storage media, it must also be in encrypted form.

Encryption of information in storage or in transit must be achieved through commercially-available products approved by the Information Security department.

Encryption keys used for ABC INTERACTIVE information are always classified as Confidential or Classified information. Access to such keys must be limited only to those who have a need to know. Unless the approval of the Information Security manager is obtained, encryption keys must not be revealed to consultants, contractors, temporaries, or other third parties.

Wireless networks in use must always be configured to employ encryption.

Transmission of data on the online system must be encrypted. Player registration and gaming transactions are continuously being transmitted on this medium, meaning that care has to be taken to protect this information.

In particular, communications established through the front-end system being used by players, as well as the communications with third parties integrated to the back-office or other similar

applications, must always be done using an appropriate secure socket layer (SSL) protocol certificate.

All back-office user and player passwords must be one-way encrypted utilising the SHA-1 encryption or similar to ensure these can never be decrypted.

All player payment related sensitive information such as player credit card numbers are stored by third party approved payment providers which are PCI-DSS certified, and not on ABC INTERACTIVE's servers.

Portable Computers and Media

Users in the possession of portable, laptop, notebook, handheld, and other transportable computers and/or media containing Confidential or Classified ABC INTERACTIVE information, must not leave these computers/media unattended at any time unless the information is stored in encrypted form.

Users in possession of transportable computers containing unencrypted Confidential or Classified ABC INTERACTIVE information must not check these computers in airline luggage systems or with hotel porters. These computers must remain in the possession of the traveler as hand luggage.

Disposal of Media & Equipment

Should any media that is no longer required due to numerous reasons, such as change in requirements, damage, inability to upgrade, non viable maintenance cost or simply replacement by new hardware must be checked by the IS department to ensure that no sensitive information is held on the device.

If the item is non-salvageable i.e. no parts can be used for other maintenance purposes, the IS department is to dispose of the equipment. The members of the IS department need to ensure that data is erased from the equipment by securely overwriting the data with 0's, while the IS manager would need to authorise the release of the equipment.

Hardware needs to be degaussed or destroyed before being disposed of.

Logs and Other Systems Security Tools

To the extent that systems software permits, computer and communications systems handling sensitive, valuable, or critical ABC INTERACTIVE information must securely log all significant security relevant events. Examples of security relevant events include users switching user IDs during an online session, attempts to guess passwords, attempts to use privileges that have not been authorized, modifications to production application software and data, modifications to

system software and data, changes to user privileges, and changes to logging system configurations.

Certain information must be captured whenever it is suspected that computer or network related crime or abuse has taken place. The relevant information must be securely stored offline until such time as it is determined that ABC INTERACTIVE will not pursue legal action or otherwise use the information. The information to be immediately collected includes the system logs, application audit trails, other indications of the current system states, and copies of all potentially involved files.

Records reflecting security relevant events must be periodically reviewed in a timely manner by computer operations staff, information security staff, or systems administration staff. The firewall has an extensive logging mechanism itself, logging all unauthorized login attempts.

Safeguarding of Applications

All systems connected to the Internet have a vendor supported version of the operating system installed. If a system is connected to the Internet, it must have the current security patches installed.

System integrity checks should be performed for both host and server systems which are housing Classified or Confidential ABC INTERACTIVE data.

Safeguarding of Networks

Firewall protection shall be put in place to safeguard the company against unauthorized intrusion attempts.

Wireless networks shall be password protected and used solely by ABC INTERACTIVE staff. Should guests wish to utilize an internet connection, a separate wireless connection shall be put in place, which is segregated from the ABC INTERACTIVE network.

Access to back-office application shall also be restricted to authorized employees and shall be given on a need to have basis. This ensures that nobody has more access rights than what is needed to carry out their duties.

The back-office application is set to automatically time out a user after one (1) hour of inactivity.

Safeguarding of Equipment

All workstations which are granted permission to access the environment will utilize the corporate anti-virus software which is deployed with every desktop/laptop build. Servers will employ anti-virus software only, and all database files will be excluded from scanning to ensure that the Remote Gaming Systems are not affected.

Servers and network devices will continually be monitored and alerts will be sent in case of any detection or other unusual occurrences. The monitoring system will produce reports to review statistical information regarding server resource usage, any changes made to network and servers, as well as capacity planning.

All employees accessing the environment are locked down via the security policy and are informed of the access levels they are granted. The devices and servers are set up so as to be able to track employees' access to these devices as well as the policy to restrict user access to data as per security policy.

The Internet firewall protects the network from unauthorised access allowing only the necessary access to internal servers via its policy-based rule set. Players are only allowed to access the remote gaming system through a web browser.

To ensure and maintain security of applications, a unique identification is assigned to each person with access, to ensure that actions taken on critical data and systems can be traced to known and authorized users. All users will be required to be identified with a unique user ID (username) before allowing them to access system components.

Communication of Policies

ABC INTERACTIVE shall ensure that employees read any required company policies and procedures upon starting work with the company and also sign an agreement to confirm compliance to these policies and procedures.

Violations

ABC INTERACTIVE users who willingly and deliberately violate this policy will be subject to disciplinary action up to and including termination.

Clear Desk Policy

Outside of regular working hours, all workers must clean their desks and working areas such that all sensitive or valuable data is properly.

Version History

Version	Date	Record of Changes
0.0	10.12.2024	Initial draft
1.0	15.01.2025	Initial release