General Games Company – ICT Security Policy

Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, General Games Company has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

Purpose

The purpose of this policy is to (a) protect General Games Company data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for company and personal use, and (d) list the company's disciplinary process for policy violations.

Scope

This policy applies to all General Games Company remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Confidential Data

General Games Company defines "confidential data" as:

- Unreleased and classified financial information.
- Customer, supplier, and shareholder information.
- Customer sales-related data.
- Patents, business processes, and/or new technologies.
- Employees' passwords, assignments, and personal information.
- Company contracts and legal records.

Device Security - Company Use

To ensure the security of all company-issued devices and information, General Games Company employees are required to:

- Keep all company-issued devices password-protected. This includes tablets, computers, and mobile devices.
- Secure all relevant devices before leaving their desk.
- Obtain authorization from the Office Manager and/or Inventory Manager before removing devices from company premises.
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or shareholders.
- Regularly update devices with the latest security software.

Device Security - Personal Use

General Games Company recognizes that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are always protected.
- Always use secure and private networks.

Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, General Games Company requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

Password Management

Passwords should not be shared with anyone, including IT support personnel, unless approved by the IT Security Specialist. All passwords are to be treated as sensitive, confidential information. If someone requests your password(s), please inform him or her that you cannot provide that information. Passwords should never be written down or stored online. Employees should try to create passwords that can be easily remembered. If you suspect an account or password has been compromised, report the incident immediately and change all related passwords. Passwords must be created and managed in accordance with these requirements:

- All passwords will expire every 90 days and must be changed.
- New passwords cannot be the same as the previous four passwords.
- Passwords must be at least eight characters in length. Longer is better.
- Passwords must contain both uppercase and lowercase characters (e.g., a-z and A-Z).
- Passwords must contain at least one number (e.g., 0-9).
- Accounts shall be locked after six failed login attempts within 30 minutes and shall remain locked for at least 30 minutes or until the System Administrator unlocks the account.

Social Media Standards

While General Games Company recognizes that we may not prohibit our employees from posting personal opinions and content on private accounts, we do expect our employees to uphold the highest level of respect and adhere to our company's privacy and security policies. This also applies to the Company's corporate accounts. Furthermore, we ask all General Games Company employees to:

- Avoid posting intellectual property and confidential company information on any social media accounts.
- Avoid discussing company-related information with customers on any social media accounts.
- Avoid sharing abusive, offensive, and/or slanderous content.
- Adhere to financial disclosure laws.

Transferring Data

General Games Company recognizes the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over General Games Company networks.
- Obtain the necessary authorization from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to General Games Company data protection law and confidentiality agreement.
- Immediately alert the IT department regarding any breaches, malicious software, and/or scams.

Disciplinary Action

Violation of this policy can lead to disciplinary action, up to and including termination. General Games Company disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.