Information Security Policy Overview

AUDIENCE: All Tinopolis Group and companies' employees.

Securing Tinopolis Group and companies ("The Company or Company") information is a shared responsibility of every Company employee. Protecting access to our data, systems and facilities ensures the confidentiality, integrity, and availability of data stored, processed, and transmitted by or on behalf of The Company, whether in physical or electronic form ("Company Information"). Systems, devices and equipment that contain or process Company information are critical to our business operations, regardless of where such systems, devices and equipment are located, and must be handled accordingly.

All information security policies, standards, procedures, and guidelines support our comprehensive security program to promote best practices for information security and must be followed at all times. It is the responsibility of every Company employee who engages third-party agents, vendors, contractors or other business partners ("Third Parties") to perform services involving access to or handling of Company Information or systems to work with Group Shared Services (IT, Legal, HR, Office Management), MSV Post and the Company, to ensure that such Third Party employ security controls and procedures that are at least as protective of Company Information and systems as those employed by The Company.

General Security Guidelines

Protect Data

Company employees must protect Company Information. It is vital to our Company and to those whose information we collect and/or store, that we maintain the highest level of integrity, ethics, and security standards. You are required to handle all Company Information in accordance with the Acceptable Use Policy and all other related Company policies, standards, and guidelines. Adequate measures must be taken to protect information from inadvertent loss or destruction and unauthorised access or handling, and to enable recovery of any Company Information that is lost (including backups and storage). If you suspect that a data incident might have taken place, you should notify the Service Desk (servicedesk@tinopolis.tv) immediately. If you suspect that the incident involves personal information, you must also immediately notify the Tinopolis Group Data Protection Manager (dataprotection.enquiries@tinopolis.tv).

Collect and store only information that is needed for business operations

Information should not be collected, shared, used or maintained unless there is a business necessity for it. Limiting data collection, sharing, use and retention to that which is reasonably necessary for legitimate business purposes is particularly important with regard to personal information. Information that is collected for valid business purposes but no longer needed should be securely disposed of in accordance with the Records Retention Policy and any other applicable policies, standards and guidelines.

Provide information on a 'Need to Know' basis

Company information is to be provided on an "as required" basis only to persons with a specific need to know. It is important to limit sharing of or access to any Company Information to the least amount of sharing or access as possible based on the business needs (e.g., do not provide an entire spreadsheet of information when only a column of names is needed). Access to applications and connectivity to the Company network should also be restricted to individuals with a specific need to know, and to only what is necessary to do their job.

Provide 'Least Privilege' access to Company Information, systems and facilities

The principle of "Least Privilege" requires that a user be given no more privilege or authority than necessary to perform a job or role. Data, system and facility access is to be provided on an as-needed basis with privileges appropriate to the context of the role.

Protect user names and passwords

All Company employees have some level of access privileges to perform their job functions. Access privileges to Company Information, systems and facilities are provided through user identification (badge number, e-mail address, account credential) and password (local or domain accounts), in accordance with job function. Company employees who have access privileges should not share, disclose, or provide Company credentials (user name, ID, email and password) to any other person, including other Company employees, for any purpose.

Company employees are expected to use appropriate safeguards to prevent the unauthorised use of assigned access credentials. Individuals are responsible and accountable for any actions performed using their access credentials.

Disciplinary Procedure

Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.