Access Control Policy

AUDIENCE: All Tinopolis Group and companies' employees.

Overview

This policy outlines the access control requirements associated with the information technology systems of Tinopolis Group and companies ("The Company or Company"). This policy is in place to protect both you and The Company and sets forth the high-level requirements that govern how access is managed and who may access The Company's information technology systems under what circumstances. Unauthorised access (e.g. using another users' credentials to access systems) of The Company's information technology systems could expose both you and The Company to risks including, but not limited to, malicious code attacks, compromise of network systems and services, as well as legal/compliance issues.

This policy applies to all information technology systems owned or leased by The Company. This policy is a subordinate policy of the Information Security Policy. It is the responsibility of every employee who engages third party-agents, vendors, contractors or other business partners ("Third Parties") to perform services involving access to The Company systems to work with members of the Information Security Work Group to ensure that such Third Parties employ security controls and procedures that are at least as protective of The Company's systems as those employed by The Company.

This policy is intended to ensure that all Company systems are properly protected against unauthorised access, while allowing authorised users (typically employees and approved Third Parties) to conduct business.

The following requirements apply to any granting of user access to a Company system:

- There must be a procedure/workflow to authorise, register, audit and de-register access for every Company system. Details of individuals' access privileges should be documented, securely maintained and reviewed on a regular basis. Individual access privileges must be promptly terminated when there is no longer a legitimate need for such access.
- Access to every Company system must be limited by the principles of least privilege, role-based access control ("RBAC"), i.e., no more access to the Company system should be given to a user than is required for the user to perform his or her job duties, and segregation of duty ("SOD"), i.e., an employee should not be able to assign your own access to the Company system without a manager's approval. For example, an employee who accesses information from a website, the individual responsible for updating the content on a website, the administrator of the application, the ID required to start a server on a server, and the network hosting administrator all have different roles that require different privileges within that Company system.
- Authentication for every Company system must at a minimum consist of a unique user ID and a unique password consistent with the Company Password Policy below, as well as multi-factor authentication where applicable and if required.
- All data that is non Public data (as defined by the Data Security Standard) will require that explicit permission be assigned, documented and approved by the data owner to each user (and denied to all others).

- Physical access to data centers, closets or cabinets that house a Company System will be granted by The Company Head of IT to employees and approved Third Parties who need to access the Company system physically. Temporary physical access to a Company system can only be granted in coordination with The Company Head of IT.
- Third Parties will not have access credentials for longer than is required to any Company system without an evaluation of required continued access.
- Administrative authentication to a Company system must be separate from day-to-day user authentication. For example, functions like user e-mail, internet access and non-privileged business functions will be separate from the installation of drivers, software, firmware, domain administration and other system administrative functions.

Password Policy

All passwords and PINs are classified as sensitive information and, as such, should not be shared with anyone.

To combat unauthorised access to your information, you are required to notify the Service Desk if you suspect that your passwords and/or PINs have been compromised, and promptly change those passwords and PINs to prevent unauthorised access to Company systems.

Password Requirements for Overall Company System Access:

- Passwords cannot be set to a null value or default (i.e., do not use default configurations on devices).
- Passwords will be rendered unreadable (i.e., encrypted) when being stored or transmitted.
- Passwords cannot be set to ‘never expire’.
- Passwords will be at minimum eight characters in length.
- Passwords cannot contain your name or parts of your full name, such as a first name.
- Passwords cannot contain words that can be found in a dictionary.
- Passwords must be changed every 90 days.
- Passwords cannot be the same as any of the last six passwords the unique ID has used.
- A user will be locked out after more than 10 inaccurate attempts and will be locked out for 5 minutes or until an administrator enables the ID.
- Each password must contain at least one character with at least three of the following four characteristics:
- Uppercase alphabetic characters (A through Z)
- Lowercase alphabetic characters (a through z)
- Numeric digits (0 through 9)
- Non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

PIN Rules

- A PIN should be a minimum of four characters in length
- A PIN should be rendered unreadable (i.e., encrypted) when being stored or transmitted.

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.