D’ANCHOR SECURITY POLICY

INTRODUCTION

This is a guideline of our organization security policy for preserving our customers data and the organization data and infrastructure.

The risk of data theft and security breaches can have a serious impact on the organization. As a result, we have created this policy to help outline the security measures put in place to ensure that data is protected.

PURPOSE

As an online commercial store that collect, store and manage data, we are prone to security attacks. This policy outlines the principles of confidentiality, integrity and availability and also guidelines that govern security measures. It also outlines the disciplinary process for policy violation.

SCOPE

This policy applies to all staff of D'Anchor, permanent or part-time workers, and/or anyone with access to company's information resources, hardware and/or software.

DEVICE SECURITY

Most employees use personal systems to access company's resources which is allowed in our organisation. However, this could cause a serious risk to the company if not done with care.

In order to protect the company against malicious attack, we have outlined various requirements:

- Ensure all personal owned devices are registered with IT
- Ensure all devices are password protected (minimum of 12 characters)
- Ensure that devices are secured before leaving the desk
- Use secure networks ONLY to log into company's accounts.
- Regularly update device to latest software
- Never disclose your password to anyone, particularly to family members, if business is conducted from home
- All personal devices should have a full-featured antivirus software

PASSWORD

Passwords are very important for personal and organisational security. A leaked password or weak password can be very dangerous to both an individual and an organisation. A password should not only be secured but also kept a secret. Here are the requirements for password protected

- Passwords must be 12 characters long
- Passwords must be a combination of alpha, numeric, and special characters
- Do not use passwords such as your name, username, birth date, nickname, relative
- Passwords must not be dictionary words
- Passwords must be changed every six months

- The same password must not be used for multiple accounts
- Passwords must not be shared with anyone, not even relatives
- Passwords must not be stored any where without encryption
- Password must be changed on any device or account that seem to be compromised
- Devices must not be left unattended to with it being password protected
- Do not use auto login or use of password managers

EMAIL

Emails have been one of the ways individuals and organisations are maliciously attacked which leads to data theft, scams and malicious software like worms and bugs. Incoming mails must be treated with utmost care due to information security risks. Therefore, employees are required to do the following:

- Do not forward confidential information without permission
- Inspect every mail thoroughly. Verify the legitimacy of the email address and sender name
- Avoid opening attachments, downloading files, and clicking on links that you are not sure of
- Do not give out your personal details such as credit cards based on a mail sent to you.
- Avoid clickbait titles and links such as offering prizes
- Look at for inconsistency such as grammatical mistakes, capital letters etc.

INTERNET ACCESS

Company's internet access and usage must be well managed. Users are provided internet access within the premises to assist in the performance of their jobs.

- Share confidential data over Company's network and not over public WIFI.
- All software used to access the internet must be part of the company's standard software approved by IT.
- All files downloaded from the internet must be scanned for viruses using the company's virus detection software.
- All employees are prohibited from using the internet to deliberately propagate any virus, worm, Trojan Horse, or any malicious program.
- If an employee accidentally connects to an inappropriate site, the employee must disconnect immediately and report the incident immediately to IT.

DISCIPLINARY ACTION

Violation of this policy can lead to disciplinary action, which could include termination.

- Unintentional or first-time violation may warrant only verbal warning
- Frequent and international violations of same act may lead to written warning, suspension and/or termination