Digipixel’s Information Systems Policy Compliance

Purpose

The purpose of this policy is to outline the acceptable use of all computer and IT equipment based in Digipixel. These rules are in place to legally protect the employees and company from risks including malicious cyber threats, compromise of network systems and services. Following the guidelines and policies below will minimize risk of facing undesirable setbacks including the theft of customer data and disruptions to service operations.

Scope

This Acceptable Usage Policy covers the security and use of all (Digipixel) information and IT equipment. This policy applies to all (Digipixel) employees, contractors and agents (hereafter referred to as ‘individuals’). This policy applies to all information, in whatever form, relating to (Digipixel) business activities and to all information handled by (Digipixel).

a. Access Control

Individuals must not:

- Leave their user accounts logged in at an unattended and unlocked computer.
- Leave their password unprotected (E.g. writing it down).
- Perform any unauthorised changes to (Digipixel) IT systems or information without the consultation and/or the approval of management (DPO - Dave).
- Attempt to access data that they are not authorised to use or access.
- Connect any non-(George’s) authorised devices to the (George’s) network or systems such as Point-of-Sales systems, PointPads, servers and other IT infrastructure.
- Store (Digipixel) data on any non-authorised (Digipixel) equipment without authorisation. E.g. storing confidential company records in your personal computer, phone or USB Storage Device.

• Give or transfer (Digipixel) data, software or data management plans to any outside person or organisation (Digipixel)

• Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done from home or at any remote location.

b. Internet and Email Usage

Individuals Must Not:

• Use the internet or email for the purposes of harassment or abuse.

• Use profanity, obscenities or derogatory remarks in communications.

• Access, download, send or receive any data (including images), which (Digipixel) considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

• Use the internet or email (Digipixel) to make personal gains or conduct a personal business.

• Share sensitive business data such as Price Lists, Business Quotations or B2B arrangements that are considered confidential business information.

• Use the internet or email to gamble.

• Place any information on the social media that relates to (Digipixel) without authorisation.

• Creating or forwarding spam and/or non-business related emails of any type.

• Forward (Digipixel) mail to personal email accounts without authorisation. For example, forwarding or removing emails from Digipixel.com.sg email accounts to your own personal hotmail account without approval of DPO Grace.

• Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.

• Opening downloaded material without scanning the file with anti-virus software.

c. Working Off-Site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left out sight. (E.g. Leaving your laptop unattended in a car)

- Care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and where available, encryption.

- DPO Grace must be aware of any company information or electronic devices taken off site.

d. Security Guidelines

Digipixel has implemented automated virus detection and virus software updates within company devices. All PCs have security solutions installed to detect and remove any virus automatically. Steps will be taken to further protect and improve the coverage of these security solutions as threats evolve.

Individuals must not:

- Remove or disable anti-virus software.

- Attempt to remove virus-infected files or clean up an infection, other than using approved (Digipixel) anti-virus software and procedures.

- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Avoiding user authentication or security of any host, network, or account.

- No plugging in unauthorized USB, CDROM, DVD that has not been cleared by the DPO.

- Scan all USB, CDROM, DVD devices before opening them using approved (Digipixel) anti-virus software.

e. Clean Desk

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be away for an extended period.

- Computer workstations must be shut down completely at the end of the workday.
- File cabinets or drawers containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.

f. Anti-Virus Guidelines

- NEVER open any files or links attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.