PIA ACCEPTABLE USE POLICY

This Acceptable Usage Policy covers the security and use of all PIA information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to employees, contractors and visitors.

This policy applies to all information, in whatever form, relating to PIA business activities worldwide, and to all information handled by the contractual agreement relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated within the PIA or on its behalf.

Individual's Responsibility

Access to the PIA IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the PIA IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any PIA IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access PIA IT system systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to PIA IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non-PIA IT system authorized device to the PIA IT network or IT systems.
- Store PIA IT system data on any non-authorized equipment.
- Give or transfer PIA data or software to any person or organization outside the PIA without the authority from the ISSM or the Information Systems Owner.

Internet and Email Conditions

Use of internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to PIA information systems, not in breach of any term and condition of employment and does not place the individual or in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

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 are considered offensive in any way, including sexually explicit, discriminatory, defamatory or material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the PIA, alter any information about it, or express any opinion, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Make official commitments through the internet or email on behalf of the PIA unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect devices to the internet using non-standard connections.

Social Media Usage

Social media serves as a common means of communication and self-expression with vast accessibility to a rapidly growing online community. However, the Cyber Innovation Center recognizes the risks of social media and how it can affect our brand, public image, core values, and overall interests of the company. Therefore, the following guidelines must be met to lay the foundational framework for guidelines and protocols. Breach of these guidelines and protocols may result in disciplinary actions and possibly termination of employment.

- Avoid speaking/posting about topics without validating it with company expertise and explicit approval from the FSO, ISSM, and Directors.
- Post only appropriate and respectful content.
- Express only personal opinions, not any of the Cyber Innovation Center.
- Avoid posting/sharing offensive, discriminatory, defamatory, derogatory, illegal, and/or false information.
- Never disclose any confidential, proprietary, or personal information relating to the Cyber Innovation Center.

Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, the PIA enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

Working Off-site

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

- Working away from the office must be in line with CIC remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely.
- Particular 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.

Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. PIA authorized storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software

Employees must use only software that is authorized by the ISSO/ISSM on PIA information systems. Software must be used in accordance with the software supplier's licensing agreements.

Telephony (Voice) Equipment Conditions of Use

Use of voice equipment is intended for business use. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

- Use voice assets for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic operators unless approved.

Actions upon Termination of Contract

All PIA equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned at termination of contract. All data or intellectual property developed or gained during the period of employment remains the property of and must not be retained beyond termination or reused for any other purpose.

It is your responsibility to report suspected breaches of security policy without delay to the CICCE IT department and the information security department. All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with disciplinary procedures.

_____

USER Date