Policies and Procedures Manual

Corporate Information Security Policies

Reference No	:	PPM-ITO-TPE-4.0
Version No	:	02
Effectivity Date	:	April 1, 2018

Prepared by:

Position / Title	Name	Signature	Date
IT Manager	Rynel Yanes		

Reviewed and Approved by:

Position / Title	Name	Signature	Date
VP for Operations	Joy Sebastian		

1.0 OBJECTIVE

1.1 To ensure the protection of the information assets owned by Open Access BPO Limited, its affiliates and its clients from unauthorized disclosure, transfer and use.
1.2 To define organization wide data classification standards.
1.3 To define acceptable use policy of information assets and computing services.
1.4 To provide a safe and secure information systems working environment for all the employees of the Organization.

2.0 SCOPE

This policy manual applies to all individuals working for Open Access BPO Limited., "The Company", including regular/probationary full-time/part-time employees, contract-based consultants, client employees, temporary agency workers, interns, trainees, business partners, and vendors) accessing the company network and information.

3.0 DEFINITION OF TERMS

IT Asset	Information Asset. Refers to a system for generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by which data is recorded, transmitted, or stored, and any procedure related to the recording, transmission, or storage of electronic data, electronic message, or electronic document.
Computer Equipment	Used in this document as pertaining to a Desktop PC set, laptop PC, IP phone, mobile phone, tablet and other peripherals used to process, transmit or store electronic data.
Confidential Information; Classified Information	Sensitive Information; client data, company information, corporate strategies, dialer leads, competitor sensitive information, trade secrets, specifications, customer lists, research data, employee PII, client financial information and/or Protected Health Information.
PII	Personally Identifiable Information. Any information that can be used to distinguish or trace an individual's identity such as Name, social security number, Tax Payer I.D., Date and Place of Birth, etc.

4.0 REFERENCES

4.1 Open Access BPO Employee Code of Conduct

5.0 POLICIES AND GENERAL GUIDELINES

The Company's information asset users are expected to be familiar with and to comply with this policy. They are also required to use their common sense and exercise good judgment while using the company information assets.

5.1 Data Classification Standards

The table below summarizes the information classification levels that is implemented by OAMPI, Inc. to identify the level of care and protection that must be applied to information assets.

Classification / Level	**Definition**	**Example**
Confidential	Causes grave damage to the mission of the organization	Client data, Strategic business plans, etc.
Sensitive	Causes damage to the mission of the organization	PII, HR and Financial Data, Medical Data, etc.
Private	Refers to data that should stay private within the organization but does not meet the Confidential or Sensitive definition.	Internal email conversations,
General	Refers to company data that does not cause damage to the mission of organization. It includes information posted in websites, brochures, or any other pubic source.	Job postings, Company overview, etc.

All company documentation, records and information assets processing and storing data should be labelled accordingly.

5.2 Internet Usage Policy

5.2.1 Consequences to violations

Violations of the *Internet usage policy* will be documented and can lead to revocation of access privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

All employees requiring Internet access are required to sign an Information Security Acknowledgement form prior to or during onboarding.

5.2.2 Usage Threats

Internet connectivity presents the company with new risks that must be addressed to safeguard the facility's vital information assets. These risks include:

5.2.2.1 Inappropriate use of Internet resources

Access to the Internet by personnel that is inconsistent with business needs or without due authorization results in the inappropriate of Internet resources. Copyright Violations, Loss of productivity, bandwidth over-utilization and unauthorized use of anonymity software is categorized under misuse of resources.

5.2.2.2 Misleading or false information

All information found on the Internet should be considered suspect until confirmed by another reliable source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

5.2.2.3 Leakage of sensitive company information or "Data Loss"

Sensitive company information includes (but is not limited to) client information, corporate financial information, Corporate Strategies and Trade Secrets, Personally Identifiable Information, Protected Health Information (PHI), Employee Medical Records, Credit Card information, etc.

5.2.2.4 Computer infection of malwares

Malware is a term with many different definitions and names like ransomware, spyware, viruses, adware, Trojans, etc. It is a software used to spy other users, gain remote connectivity and control, display advertisements, and other software activities that allow the computer to work for the malware author's benefit.

5.2.3 User Services

Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

5.2.3.1 Allowed Internet Services

Internet access is for business purposes only. Capabilities for Internet services will be provided to users based on approved business unit Internet access baseline as enumerated below:

- Corporate emails (Google Apps for Business, Amazon hosted internal email)
- Web browsing.
- Messaging tools and apps.
- Client-based remote connectivity apps (VPN, SSLVPN, etc.)
- Cloud-based VoIP / Internet Telephony.
- Corporate forward proxy (hosted in USColo).
- Other Internet-dependent services required and approved by the top management via a Security Exception documentation.

Management reserves the right to add or remove Internet services as business needs change or conditions warrant. **All other unlisted access will be considered as "unauthorized access" to/from the Internet and hence, shall be prohibited.**

5.2.3.2 Request and Approval

Other internet resources or services prohibited by this policy manual, as deemed necessary to complete a business unit task or function, can be superseded by the request and approval of the top management via a Security Exception Documentation.

5.2.3.3 Removal of Internet access privileges

Internet access will be discontinued upon termination of employment, completion of contract, end of service of non-employee, or temporary or permanent disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer the original access will be discontinued, and only reissued if necessary and a new request for access is approved.

5.2.4 Usage Policies

5.2.4.1 Internet access provision

Access to the Internet will be approved and provided as business needs are identified. Internet services will be granted based on an employee's current job responsibilities. If an employee moves to another business unit or changes job functions, a new set of Internet access privilege will be provided.

User Internet access requirements will be reviewed periodically by company departments to ensure that continuing needs exist.

5.2.4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department. Acceptable use of the Internet for performing job functions include but are not limited to:

- Communication between employees and non-employees for business purposes.
- Fulfillment of production tasks with the use of client/vendor provided tools and applications.
- Research and reference.
- Information validation / Verification.
- Multimedia reference for training, creation of multimedia materials, and other activities for business purposes.

5.2.4.3 Personal Usage

Using company Internet for personal purposes, without approval from the user's manager and the IT department, can be considered cause for disciplinary action up to and including termination.

All employees using the company Internet should be aware that the company network creates an audit log of all inbound and outbound Internet traffic created, and is periodically reviewed.

5.2.4.4 Prohibited Usage

Internet activities that fall under the following description is prohibited:

- Access, acquisition, storage, and dissemination of data which is non-business related, illegal and/or pornographic.
- Dissemination or proliferation of false or libelous or damaging information to the reputation of the Company.
- Conduct of a business enterprise, political activity, engaging in any form of intelligence collection from the Company facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.
- Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of client and/or personnel file information, and accessing information that is not needed for the proper execution of job functions.
- Misusing, disclosing without proper authorization, or altering client or personnel information. This includes making unauthorized changes to a personnel file or sharing the company client database or personnel data with unauthorized personnel.
- Deliberate pointing or hyper-linking of corporate internet resources and sites to other Internet sites whose content may be inconsistent with or in violation of the aims or policies of the Company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, compliance, local, state, national or international law including without limitations government control laws and regulations.
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Transmission of any proprietary, confidential, or otherwise sensitive company and/or client information without the proper controls and due authorization.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

- Access to non-work related audio and/or video streaming.
- Unauthorized access to Social Media Sites.
- **Accessing of known restricted websites**.
- **Accessing and/or usage of proxy sites/apps**.
- Circumventing of Internet access restrictions
- Usage for the purpose of the transmission of commercial or personal advertisements, solicitations, or promotions.

Unless specifically authorized under the provisions of section 5.2.4.2, the following activities are also strictly prohibited:

- Unauthorized downloading of any files (regardless of the type) without authorization from the Campaign Manager and approval from the IT Operations.
- Access to online gaming applications / online gaming sites.
- Participation in any on-line contest or promotion.

Bandwidth, both within the company and in connecting to the Internet, is a shared and finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

5.2.4.5 Intellectual Property on the Internet

The company strongly supports strict adherence to software license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of copyrighted materials on the Internet is forbidden unless this is both reasonable and customary. This notion of "fair use" in this context is in keeping with international copyright laws.

5.2.4.6 Review of Internet access information

All Internet access logs and browsing history in computer equipment are reviewed regularly and cleared as needed. This process is necessary to prevent the anonymous exchange of information inconsistent with the company business.

5.2.4.7 Expectation of Privacy

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

The Company reserves the right to backtrack, examine, trace, monitor all Internet access transactions at any time and without notice. This ensures compliance with the company information security policies and this assists with the management of company information systems.

5.3 Computer Equipment Usage Policy

Computer equipment usage policy are not to impose restrictions that are contrary to the company's established culture of openness, trust and integrity. This is committed to protecting the company's employees, partners and clients from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, production application systems, network systems, voice systems, storage media, network accounts providing email, web browsing, and the like, are the property of the Company. These systems are to be used for business purposes in serving the interests of the company, for the clients and customers in the course of normal operations.

An effective Information Security program is a collaborative effort in the organization involving the participation and support of every employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and policies, and to conduct their activities accordingly

5.3.1 Consequences to violations

Violations of the computer equipment usage policies will be documented and can lead to revocation of access privileges and/or disciplinary action up to and including payment for the damages and/or termination (See Employee Code of Conduct).

5.3.2 Usage threats

5.3.2.1 Physical Damage

Any physical condition that renders the Internet/Intranet/Extranet-related systems functionality into an unusable, security compromised or degraded state. Cracks, dents, deep scratches, deformity on the chassis, casing or exterior of the computer equipment included.

Actions resulting to hardware damage such as inappropriate computer use, liquid spills, unauthorized chassis tampering/opening, unauthorized computer accessories/peripherals transfer and use, and computer equipment negligence fall under this category.

5.3.2.2 Loss of computer services

This includes hardware or software failure such as power supply or electrical failure due to improper use, failure of peripheral accessories, computer boot failure, non-launching of applications, unintended license revocations, denial of access to productivity tools, etc.

5.3.2.3 Compromise of information

Unauthorized access, transmission and/or damage to any data stored in a computer.

5.3.2.4 Infection of malwares

5.3.3 General Usage

5.3.3.1 Employees are responsible for exercising good judgment regarding the reasonableness of Internet/Intranet/Extranet-related systems usage. Individual departments/campaigns are responsible for creating guidelines concerning use of the Internet and/or local computer equipment supplementary to this policy manual. If there is any uncertainty, employees should consult their immediate superior or course clarifications to the IT Department.

5.3.3.2 Authorized individuals within the company (such as the IT Department) may monitor computer equipment, systems and network traffic at any time.

5.3.3.3 Removal of usage privileges

Usage privileges of computer equipment to access Internet/Intranet/Extranet related-systems will be discontinued upon termination of employee, completion of contract, end of service of non-employee, or temporary or permanent disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer, the original access will be discontinued, and only reissued if necessary and a new request for such access is approved.

5.3.4 Usage Policies

5.3.4.1 Employees should take all necessary steps to prevent unauthorized access to company confidential information contained in the Internet/Intranet/Extranet-related systems.

5.3.4.2 Accessing confidential information from the Internet/Intranet/Extranet-related systems is only allowed as required by the campaign operations and/or as requested by the campaign/operations manager.

5.3.4.3 Storage of confidential information on removable storages, laptop/ desktop computers and mobile devices is strictly prohibited (in highly secured cases, USB storage function of computer equipment is disabled by default). Should a requirement for storage arise, an authenticated and encrypted central storage is provided by the IT Department.

5.3.4.4 Transfer of classified information from Internet/Intranet/Extranet-related systems is only allowed if duly approved by the campaign/operations manager and provided that encryption will be used in the transmission of data.

5.3.4.5 Electronic deletion of confidential information from all computer equipment should be done in such a way that it cannot be recovered.

5.3.4.6 Sharing of login account information for any computer equipment is strictly prohibited. Employees are responsible for the security of their login username and passwords and shall make sure to keep it from others' knowledge.

5.3.4.7 All Desktop and Laptop computers are secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off.

5.3.4.8 The IT Department is the only authorized body to install or uninstall computer hardware and software. All requests or requirements to add hardware or software should be coursed through the IT Department.

5.3.4.9 The Company management through the IT Department reserves the right to access, remove, confiscate or uninstall unauthorized hardware (including unauthorized computer peripherals and accessories) or software found in a computer equipment.

5.3.4.10 The user is fully responsible and accountable for the computer access, computer equipment and all attached parts, components, peripherals and accessories.

5.3.4.11 Any access breach and damage to the computer equipment should be immediately reported to the immediate superior or to the IT Department.

5.3.4.12 User's communications should reflect high ethical standards, mutual respect, and civility.

5.3.4.13 Prohibited Use

5.3.4.13.1 TBD – intentionally left blank

5.3.4.13.2 Putting up / Applying stickers, marks in any part of the computer hardware and chassis.

5.3.4.13.3 Unauthorized dismantling, removal or replacement of any part, component, peripheral or accessory of the computer equipment.

5.3.4.13.4 Removal or Tampering of the company Asset Tag.

5.3.4.13.5 Misuse or abuse resulting to damage to any part, component, peripheral or accessory of the computer equipment.

5.3.4.13.6 Unauthorized transfer of any part, component, peripheral or accessory of a computer equipment setup.

5.3.4.13.7 Intentional or unintentional Installation of unauthorized applications.

5.3.4.13.8 Introduction of malicious programs, spyware and viruses into the network or servers.

5.3.4.13.9 Disclosing account password to others or allowing use of account by others.

5.3.4.13.10 Attempting to circumvent, assisting others to circumvent, or requesting others to circumvent any security settings, measure or technical access control configuration applied to the computer equipment.

5.3.4.13.11 Circumventing user authentication or security of any host, network or account.

5.3.4.13.12 Interfering with or denying service to any user other than the employee's computer equipment.

5.3.4.13.13 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, tamper, or disable, a user's session, via any means.

5.3.4.13.14 Accessing of confidential information without due authorization.

5.3.4.13.15 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, forged routing information for malicious purposes, and/or similar kinds of attacks.

5.3.4.13.16 Unauthorized data interception.

5.3.4.13.17 Storing of non-business related files such as images, videos, music, games, etc.

5.3.4.13.18 Running of unauthorized or prohibited executables including portable applications (e.g. Spotify, torrent clients, etc.)

5.3.4.13.19 Usage of the computer equipment that violates other policies stated in the OAMPI Inc. Employee code of conduct.

5.3.4.13.20 Usage of computer equipment that supports criminal and illegal activities. Criminal and illegal use may involve, but is not limited to, unauthorized access, deliberate data leakage, intentional corruption or misuse of computer resources, theft, obscenity, pornography, and sexual harassment.

5.3.4.13.21 Usage for the purpose of the transmission of commercial or personal advertisements, solicitations, or promotions.

5.3.4.13.22 Unauthorized modification of computer equipment system settings without due authorization from IT.

5.3.5 Computer login credential policies (Domain login credentials)

5.3.5.1 Unauthorized Sharing/Disclosing of computer login credential is strictly prohibited.

5.3.5.2 Writing down or electronically listing the computer login credentials is strictly prohibited.

5.3.5.3 The use of password vault/manager applications are not allowed.

5.3.5.4 The computer login password must be atleast 7 characters in length and contain atleast 1 numeric and 1 alphanumeric character.

5.3.5.5 The computer login password expires and must be changed atleast every 90 days.

5.3.5.6 Recycling / reuse of past 4 computer login passwords is not allowed.

5.3.5.7 Employee must change the temporary computer login password provided by the IT Operations on the first login.

5.3.6 Intellectual Property

5.3.6.1 Unauthorized duplication of company-licensed commercial and proprietary applications is strictly prohibited.

5.3.6.2 All applications or software installed in a computer equipment should be legally licensed.

5.3.6.3 Making copies of copyrighted materials is forbidden unless this is both reasonable and customary. This notion of "fair use" in this context is in keeping with international copyright laws.

5.3.7 Expectation of Privacy

5.3.7.1 While the Company's direction desires to provide a reasonable level of privacy, **users should be aware that the data they create on the corporate systems remains the property of the Company.** Because of the need to protect the Company's computer equipment network, the Company reserves the right to examine all personal file directories, browser access history, and other information stored on any company computer equipment, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

5.4 Wireless Access Policies

5.4.1 Consequences to violations

Violations of the Wireless Access policy will be documented and can lead to revocation of Wireless access privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

5.4.2 Usage Threats

5.4.2.1 Rogue Access Points

Rogue Access Point (Rogue AP) is a wireless access point installed on a wired enterprise network without authorization from the IT Operations. It can be used to launch man-in-the-middle attacks or denial of service.

5.4.3 Acceptable use

5.4.3.1 Wireless Access is only provided to members of the executive management, business unit heads and back office personnel.

5.4.3.2 Wireless Access may also be provided to employees and/or vendors, partners and visitors as authorized by the top management via the Corporate Wireless Network with Captive Portal for authentication.

5.4.4 Prohibited use

5.4.4.1 Unauthorized attempts to connect to the company wireless network.

5.4.4.2 Usage of authentication cracking tools.

5.4.4.3 Unauthorized usage of wireless sniffing tools and applications.

5.4.4.4 Placing, usage or operating of an unauthorized wireless device within the company premises.

5.4.4.5 Accessing of productions / operations client tools and applications via the wireless network.

5.5 Door Access Policies

5.5.1 Consequences to violations

Violations of the Door Access policy will be documented and can lead to revocation of Production floor access privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

5.5.2 Usage Threats

5.5.2.1 Unauthorized personnel entry.

5.5.2.2 Non-badge entry or tailgating.

5.5.2.3 Piggy-backing.

5.5.3 Acceptable use

5.5.3.1 All company employees are required to badge in to door-in proximity device upon entry to the production floor and badge out to door-out proximity device upon exit.

5.5.3.2 ID Badge with RFID must be worn at all times inside the production floor.

5.5.4 Prohibited use

5.5.4.1 Tailgating and Piggy-backing are strictly prohibited.

5.5.4.2 Non-badge entries in the production floor should be authorized and logged by the designated security guard.

5.5.4.3 Sharing / Lending of ID Badge (Piggy-backing).

5.5.4.4 Unauthorized use of other's ID Badge.

5.6 Email Policies

5.6.1 Consequences to violations

Violations of the email policy will be documented and can lead to revocation of email privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

5.6.2 Usage Threats

5.6.2.1 Malware Attachments

This comes in a form of archived (Zipped) attachments or unsuspecting regular documents embedded with malwares that attach to the computer equipment when opened.

5.6.2.2 SPAM

Junk email that can affect email system availability. This looks like a regular email but contains attached malware or advertisements.

5.6.2.3 Phishing

Emails that lure its recipients to spoofed websites and tricking them to provide personal information such as Credit Card Numbers, Bank Account info etc.

5.6.2.4 Client information leakage.

5.6.2.5 Intentional or unintentional unauthorized email communications.

5.6.3 Usage Policies

5.6.3.1 Unacceptable use

5.6.3.1.1 Sharing or disclosure of email login information and account details to unauthorized users.

5.6.3.1.2 Creation or distribution of any non-business related, disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

5.6.3.1.3 Distribution and/or storage of any confidential or sensitive Company and/or client information without due authorization.

5.6.3.1.4 Sending of non-business related, chain letters or joke emails from the company email account or from a personal account to the company email.

5.6.3.1.5 Using of company email address to subscribe to social networking sites, jobsites, professional networking sites, and other websites or applications without consent and approval of the Management.

5.6.3.1.6 Mass mailings to/from the company without approval from the management.

5.6.3.1.7 Sending of a single email with more than 25 recipients without due authorization.

5.6.3.1.8 Unauthorized sending of more than 20 emails within 60 minutes.

5.6.3.1.9 Sending unauthorized emails to the existing and prospect clients.

5.6.4 Email login credential policies

5.6.4.1 Unauthorized Sharing/Disclosing of email login credential is strictly prohibited.

5.6.4.2 Writing down or electronically listing the email login password is strictly prohibited.

5.6.4.3 The email login password must be atleast 7 characters in length and contain atleast 1 numeric and 1 alphanumeric character.

5.6.4.4 The email login password must be changed atleast every 90 days.

5.6.4.5 Employee must change the temporary email login password provided by the IT Operations on the first login.

5.6.5 Privacy Expectation

5.6.5.1 The company employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. The company reserves the right to monitor messages without prior notice. The company is, however, not obliged to monitor all email messages.

5.6.5.2 The Company reserves the right to access and examine email at any time without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

5.7 Central File Storage

Central File Storage service is provided to the users so they can transfer, collaborate, share and store files securely over the network. This service is only provided to business units approved to have such usage.

5.7.1 Consequences to violations

Violations of the Central File Storage will be documented and can lead to revocation of storage privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

5.7.2 Threats

5.7.2.1 Inappropriate use such as storage of non-business related files;

5.7.2.2 Intentional or Unintentional Data deletion.

5.7.2.3 Malware infection.

5.7.3 Prohibited Usage

5.7.3.1 Storing of non-business related files such as images, movie files, music files, games, applications, etc.

5.7.3.2 Storing of files containing client confidential data such as credit card information, PII, SSN, medical information, etc.

5.7.3.3 Storing of any file longer than the specified file retention scheduled per Department/Campaign.

5.7.3.4 Circumventing folder access restrictions.

5.7.3.5 Unauthorized navigating, viewing, deleting and modifying contents of a file or folder.

5.7.3.6 Unauthorized decryption of stored files.

5.7.4 Intellectual Property

5.7.4.1 Unauthorized storage of company-licensed commercial and proprietary applications is strictly prohibited.

5.7.4.2 Making copies of copyrighted materials is forbidden unless this is both reasonable and customary. This notion of "fair use" in this context is in keeping with international copyright laws.

5.7.5 Privacy Expectation

The company employees shall have no expectation of privacy in anything they store in the Central File Storage. The company reserves the right to monitor all file logs and access without prior notice.

5.8 IP Telephony

5.8.1 Consequences to violations

Violations of the IP Telephony usage policy will be documented and can lead to revocation of telephony privileges and/or disciplinary action up to and including termination (See Employee Code of Conduct).

5.8.2 Usage Threats

5.8.2.1 Voice Phishing (Vhishing)

The practice of using social engineering over the telephone system to gain access to private personal and financial information.

5.8.3 Acceptable use

5.8.3.1 IT Operations test calls.

5.8.3.2 Authorized calls with prospect and existing clients, vendors and partners.

5.8.3.3 Internal communication.

5.8.4 Prohibited Usage

5.8.4.1 Scam and Prank calling.

5.8.4.2 Unauthorized international outbound dialing.

5.8.4.3 Intentional or unintentional non-hanging up of hard-phone handset.

5.8.4.4 Internal or External calls for personal purposes.

5.8.5 Privacy Expectation

The company employees shall have no expectation of privacy in all calls made using the company telephony system. The company reserves the right to review all numbers called and call recordings without prior notice.