

APP Group and Its Subsidiaries

Computer Usage and Access Policy

General Terms and Conditions on Computer Usage

The computer resources are the property of APP Group and its subsidiaries (the "Company") and may only be used for legitimate business purposes. Users (which includes all employees, independent contractors, consultants, temporary workers and other persons or entities who use the computer resources) are provided access to the computer resources (which includes but is not limited to host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, software, data files, and all internal and external computer and communication networks e.g., Internet, commercial online services, value-added networks, e-mail systems) to assist them in the performance of their job.

To ensure that the Company's computer resources are used properly by all Users, the Company has created this Computer Usage and Access Policy (the "Policy"). The rules and obligations described in this Policy apply to all Users, wherever they may be located. All Users are responsible for using the Company's computer resources and the Internet professionally, lawfully and ethically. Violations will be taken very seriously and may result in disciplinary action, including possible termination, and civil and criminal liability. This policy is also referred to APP Group Corporate Information Technology

Computer Resources Use Limitations

Prohibited Uses. Without prior written permission from the Company, the Company's computer resources may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, self-replicating programs, etc.), political material, pornographic text or images, or any other unauthorized materials.

Users may not use the Company's Internet connection to download games or other entertainment software (including screen savers), or to play games over the Internet. Additionally, Users may not use the computer resources to display, store or send by email or any other form of electronic communication (such as bulletin boards, chatrooms, Usenet groups, etc.) material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory or otherwise inappropriate or unlawful. Anyone receiving such materials should notify their supervisors

Users are also prohibited from tampering with the Company's computer resources. When any computer resource is no longer required, Users and/or their supervisors shall return such computer resources to the IT Department. Prior notification to the IT Department must be made before any re-location of computer resources is made.

Illegal Copying. Users may not illegally copy material protected under copyright law or make that material available to others for copying. Users are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material they wish to download or copy. Unless the Company's prior express written permission is sought, Users are not permitted to agree to a license or download any material for which a registration fee is charged.

Communication of Trade Secrets. Unless expressly authorized to do so, Users are prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information belonging to Company. Unauthorized dissemination of such material may result in severe disciplinary action and substantial civil and criminal penalties.

Duty not to Waste or Damage Computer Resources

Accessing the Internet. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to the Company's computer network must do so through an approved Internet firewall or other security device. Passing the Company's security device by accessing the Internet directly by modem or other means is strictly prohibited unless prior written approval from the Company has been obtained.

Virus detection. Files obtained from sources outside the Company, including disks brought from home; files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to e-mail, and files provided by customers or vendors, may contain dangerous computer viruses that may damage the Company's computer network. Users should never download files from the Internet, accept e-mail attachments from outsiders, or use disks from non-Company sources, without first scanning the material with Company-approved virus checking software. Users are responsible for notifying their supervisor and the IT Department immediately if they suspect that a virus has been introduced into the Company's network.

Frivolous Use. Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, Users must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-business-

Monitoring of computer usage and access

The Company has the right to monitor, investigate, block and record User's activities using the Company's computer resources. Data created or stored in the Company's computer system belongs to the Company and as such must be treated with proper security and confidentiality in accordance with the Policy. In the event of any suspected or proven violations, the Company reserves the right to revoke

prior notice and the User will be subject to disciplinary action, including possible termination, civil and/or criminal liability.

General Terms and Conditions on use of PIN

The Company provides Users with a PIN (Personal Identification Number) in the form of User Account, password etc. for accessing its computer resources. All Users must comply with the following conditions:

1. All first time Users will be provided with a temporary PIN. Such Users shall immediately change their PIN on first accessing the computer network.
2. Each PIN will have a certain validity period. The validity period will expire on the Users being transferred from their current job position, relieved of their current duties, their contractual services being terminated and/or their ceasing to be in the Company's employ. All Users must notify their supervisors and the IT Department on any of the above changes.
3. All security tokens that have been issued remain the property of the Company. It should be surrendered upon the expiration of the User's access validity period and returned to the Company before such User's departure.
4. All Users shall not reveal or lend their PIN and its accompanying token to any persons or entities. If the PIN is exposed or suspected to be exposed or the accompanying security token is lost, Users must immediately notify their supervisors and the IT Department.
5. Any use of unauthorized IP addresses, creation of unregistered e-mail address, masquerading of another User's identity, use of another's password, tapping of the Company's network transmission, creation of unauthorized and unsecured servers or peer-to-peer file sharing which exposes the Company's information to risk is strictly prohibited.

Amendments

The Company reserves the right to amend or revise the Policy from time to time, as and when the need arises and without prior notification. Users will be provided with copies of all amendments and

Acknowledgement of Understanding

I have read and agree to comply with the terms of this Policy governing the use of Company's computer resources.

Employee

Electronically signed by:
NAUFAL DZAKI

Date :16/7/2025

Name :NAUFAL DZAKI