



AMBC Technologies Pvt Ltd.

Information Technology Usage Policy

PURPOSE

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by AMBC and to reduce the risk of acquiring malware infections on computers operated by AMBC

SCOPE

This policy covers all computers and servers operating in AMBC

PROCEDURE

This policy must be acknowledged by each User/Employee of AMBC.

POLICY

Removable media may not be connected to or used in computers that are not owned or leased by the AMBC without the explicit permission of the IT and Infrastructure Team. Sensitive information should be stored on removable media only when required in the performance of your assigned duties or when providing information required outside of the organization. When sensitive information is stored on removable media, it must be encrypted by the AMBC Acceptable Encryption Policy. Exceptions to this policy may be requested on a case-by-case basis by AMBC.

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

INTERNET USAGE POLICY:

This Internet Usage Policy applies to all employees of AMBC who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of AMBC is permitted and encouraged where such use supports the goals and objectives of the business. However, access to the Internet through AMBC is a privilege and all employees must adhere to the policies concerning Computer, Email, and Internet usage. Violation of these policies could result in disciplinary and/or legal action leading up to and including termination of employment. Employees may also be held personally liable for damages caused by any violations of this policy. All employees are required to acknowledge receipt and confirm that they have understood and agree to abide by the rules hereunder.

COMPUTER, EMAIL, AND INTERNET USAGE:

- Company employees are expected to use the Internet responsibly and productively. Internet access is limited to job-related activities only and personal use is not permitted
- Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role
- All Internet data that is composed, transmitted, and/or received by AMBC's computer systems is considered to belong to AMBC and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties



- The equipment, services, and technology used to access the Internet are the property of AMBC and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections
- Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images
- All sites and downloads may be monitored and/or blocked by AMBC if they are deemed to be harmful and/or not productive to business
- The installation of software such as instant messaging technology is strictly prohibited
- Disclosing official email IDs on the social network is prohibited
- Unique Login Id and Password - Access to Company Resources is controlled using a unique login ID and a password. Users should protect their passwords from becoming known by anyone else, including IT personnel. If users believe that their passwords have become known to someone else, they must change their passwords as soon as practical.

UNACCEPTABLE USE OF THE INTERNET BY EMPLOYEES INCLUDES, BUT IS NOT LIMITED TO:

- Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via AMBC's email service
- Using computers to perpetrate any form of fraud, and/or software, film, or music piracy
- Stealing, using, or disclosing someone else's password without authorization
- Downloading, copying, or pirating software and electronic files that are copyrighted or without authorization
- Sharing confidential material, trade secrets, or proprietary information outside of the organization
- Hacking into unauthorized websites
- Sending or posting information that is defamatory to the company, its products/services, colleagues, and/or customers.
- Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Passing off personal views as representing those of the organization

If an employee is unsure about what constituted acceptable Internet usage, then he/she should ask his/her supervisor for further guidance and clarification

All terms and conditions stated in this document apply to all AMBC's network and Internet connection users. All terms and conditions as stated in this document reflect an agreement of all parties and should be governed and interpreted by the policies and procedures mentioned above. Any user violating these policies is subject to disciplinary actions deemed appropriate by AMBC'.

WORK FROM HOME POLICY:

working from home policy is provided to the employees, our company expecting the following from our employees. Mark the Attendance daily in the "AMBC Timesheet Application" as per their scheduled working hours and attend all the scheduled meetings without fail and all the deliverables should be completed.

The IT department or Company shall provide the home-based office setup devices (Laptops Headphones and chargers). IT department shall not provide the physical setup of the home-based office



(Laptop Desk and Office Chair etc.), but it shall provide information about options available and telephone assistance where possible. The local or corporate IT department is not responsible for support of the home office Internet or phone connection, or non-company provided devices. It is expected that these services (Modems and Dongles etc.) or devices will be supported by the service provider/manufacturer.

Asset and Hardware and Software Checklist:

Refer to the “Computer Policy” document. Asset details, Hardware, Software, etc. details are maintained under “Computer Policy”

Asset Damage or Loss: In case of negligence the company has every right to deduct it from the employee’s Salary. Employees/Contractors are responsible for the IT assets assigned to them. In case of damage or loss, they will be responsible for either replacing or repairing.

Remote Access Control: Remote workers must use a remote computer for Company activities unless this same computer runs an access control system approved by the IT Department. All Employee’s remote access to Company or Client networks must be made through approved Remote Access points that are controlled by the IT Department. After a remote worker has completed a remote session with Company computers, the worker must log off and then disconnect, rather than simply disconnecting. Workers using remote communications facilities must wait until they receive a confirmation of their log-off command from the remotely connected Company machine before they leave the computer using.

Changes to Configuration Hardware and Software: Remote working computer equipment supplied by Company must not be altered or added to in any way without prior knowledge and authorization from the IT Department. Employees must not change the operating system configuration or install new software. If such changes are required, they must be performed by an IT Department person with remote system maintenance software.

Backup: The work-from-home user is responsible to safeguard important office data by performing regular backups weekly once. The local IT department can recommend appropriate backup methods (Backup Method: OneDrive) to keep Important files in the OneDrive folder for Automatic backup. work from a user has complied with backup policy.

INFORMATION SECURITY:

The IT department attempt to keep Company Resources stable and secure through various methods. Users are expected to help to maintain this security. A user should not provide a computer account or network information unless the user is certain that the requester is a current member of the local or corporate IT department. If a user receives a request for information by email. Users can contact their local IT department to verify the identity of the person who is requesting the information.

Note: Users should notify the IT department immediately if a company device is lost.

MOBILE PHONE USAGE POLICY:

- All the employees are advised to keep their mobile phones in “SILENT MODE” on office premises
- Employees are not allowed to use mobile phone cameras or microphones inside the office premises
- Employees can make brief personal calls away from the workspace in case of emergency.
- Watching videos, playing games, or using social media applications during work hours is strictly prohibited.



- The phone is company property, if the phone was damaged or if the employee lost it they will be responsible for either replacing or repairing it.
- They must return the phone once their employment ends.
- You reserve the right to withdraw or replace their phone.

TELEPHONE USAGE POLICY:

Personal telephone calls are not prohibited, their frequency, duration, and volume should not interfere with ongoing work duties nor distract fellow employees. This includes both incoming and outgoing telephone calls. Abuse of this privilege may lead to disciplinary action.

Employees are not permitted to make personal long-distance telephone calls using the company's telephones except in emergencies.

REMOVABLE STORAGE DEVICE POLICY:

Removable media is a well-known source of malware infections and has been directly tied to an organization's loss of sensitive information.

USER COMPLIANCE:

I understand and will abide by this "Internet Usage Policy and Mobile Phone Usage Policy and work from home usage Policy and Computer Policy". I further understand that should I commit any violation of this policy, my access privileges may be revoked, disciplinary action and/or appropriate legal action may be taken.

Employee ID & Name

Employee Signature