TECHRADIUS
We Beyond The World

DATA SECURITY

DESKTOP USAGE

- ✓ All computers are provided for business purposes only and shall not be used for personal activities.
- ✓ The personal passwords shall be maintained confidential and work group passwords shall be shared only within the members of the group.
- ✓ Privacy of other users should be respected. Users should not seek or reveal information on, obtain copies of, or modify files, tapes, or passwords belonging to other users, nor may the user misrepresent others.
- ✓ Not to install or remove or change any devices/drives in the desktops.
- ✓ Not to disable the Antivirus software and other administrative software running on the desktops.
- ✓ Personal CD, floppies, Laptops, Flash Drives and other storage and processing Medias should be used only after prior authorization from the Work Group head.
- ✓ Not to engage in abusive or improper use of computer resources, which includes, but is not limited to, misuse of system/operator privileges, tampering with equipment and unauthorized removal of equipment components.
- ✓ Not to attempt to circumvent the security of the network, or other systems on the network either on- or off-campus. Do not conduct or permit "cracker" activities. Do not run "packet sniffers" on network.
- ✓ Distribution of computer viruses, Trojan horses, worms, or any other malicious software is not permitted.
- ✓ Not to use mobile phones or other related medium to discuss customer/ project related information in public places and will use them to respect and show courtesy to others.

INTERNET USAGE

The Company, IT Resources includes access to the Internet for business purposes and is shared among the employees. Personal use of the Internet to access multi-media such as streaming video or music, or for the download of personal Content is not permitted.

- ✓ 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.
- ✓ Using IT Resources to share personal files or allow unauthorized access to download files is strictly prohibited.

- ✓ The Company controls and monitors access to its IT Resources by assigning Users with Credentials. Users are required to keep these Credentials confidential and must not share the information with any other User or other party except the System Administrator. Under no circumstance shall any Credentials be communicated in whole with user identification and password within an Electronic Mail message.
- ✓ Not to engage or attempt to misuse or abuse the usage of internet access provided.

SOFTWARE INSTALLATION

- ✓ Employee must not install or delete Software without written approval from the System Administrator. Software shall not be copied for personal use, except as authorized by Company licensing agreements. Any unauthorized installation of Software and associated Content may be removed with no advance notice.

EMAIL USAGE

- ✓ Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted only to, the use of vulgar or harassing language/images.
- ✓ All Internet data that is composed, transmitted and/or received by Techradius Hitech Pvt. Ltd. computer systems is considered to belong to Techradius Hitech Pvt. Ltd. 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 data / equipment, services and technology used to access the Internet are the property of Techradius Hitech Pvt. Ltd. and company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent or received through its online connections.
- ✓ Not to involve in non-repudiation, falsification or misuse or Email facilities provided, for use other than business purposes.

Techradius Hitech Pvt. Ltd. (OPC) reserves the rights to monitor and check the activity in individual systems, its configurations and software installed. Any user found to have violated this policy would be subject to disciplinary action.