Acceptable Use of Assets

Idexcel's intentions for publishing an Acceptable Use of Assets are not to impose restrictions that are contrary to organization's established culture of openness, trust and integrity. Idexcel's is committed to protecting Idexcel's employees, partners and the company 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, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Idexcel. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

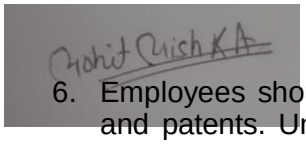
Effective security is a team effort involving the participation and support of every Idexcel employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

General Use and Ownership

1. While Idexcel's network administration 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 Idexcel.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within Idexcel may monitor equipment, systems and network traffic at any time.
4. Idexcel reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Propriety Information

1. Employees should familiarize themselves with and adhere to the policies and guidelines set forth by the organization.
2. Assets should be used only for authorized purposes and within the scope of the user's responsibilities. Employees should refrain from using assets for personal gain, unauthorized activities, or activities that may violate laws, regulations, or ethical standards.
3. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either Restricted, Confidential, Internal and public as defined by organization's Information classification guidelines. Employees should take all necessary steps to prevent unauthorized access to this information.
4. Employees are responsible for safeguarding assets from theft, loss, damage, or unauthorized access.
5. Passwords and account details are confidential and do not share to others. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed once in every 45 days and user level passwords should be changed 45 days.



6. Employees should respect intellectual property rights, including copyrights, trademarks, and patents. Unauthorized reproduction, distribution, or use of copyrighted materials is generally prohibited.

7. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off when the host will be unattended.
8. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Organization Security Policy”.
9. Employees should respect the privacy and confidentiality of data stored or processed using the assets. They should handle sensitive information in accordance with applicable data protection laws and organizational policies.
10. Employees are responsible for physical security of the devices, and they shall replace the device with same make, brand and configuration or reimburse the current cost of the device in case the device is lost or damaged.
11. Lost or stolen mobile devices must be reported to HR & IS teams immediately.
12. Employees should promptly report any security incidents, breaches, or suspected policy violations to the appropriate authority within the organization. This helps maintain the integrity and security of the assets.
13. Postings by employees from an Idexcel email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Idexcel unless posting is during business duties.
14. All hosts used by the employee that are connected to the Idexcel Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
15. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Idexcel authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Idexcel-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Idexcel.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Idexcel or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using an Idexcel computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Idexcel account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. 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, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to IS Support is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Accessing chat rooms or news groups without specific authorization from the concerned Project Manager or IS Team. This includes, but is not limited to Online Web chat rooms, Instant messenger chat, etc.
16. Using the Company's computers, networks or Internet services for any illegal activity or activity that violates other policies, procedures and/or company rules. This includes, but is not limited to pornographic materials, threats, or gambling.
17. Providing information about, or lists of, Idexcel employees to parties outside Idexcel.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, Microsoft teams chat, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Idexcel's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Idexcel or connected via Idexcel's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Blogging and Social Networking

1. Blogging and social networking using Facebook, Myspace, Twitter, Orkut and mail groups by employees, whether using Idexcel's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of Idexcel's systems to engage in these activities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Idexcel's policy, is not detrimental to Idexcel's best interests, and does not interfere with an

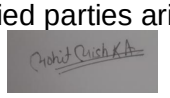
employee's regular work duties. Blogging and social networking from Idexcel's systems is also subject to monitoring.

2. Idexcel's Confidential Information policy also applies to blogging and social networking. As such, Employees are prohibited from revealing any Idexcel confidential or proprietary information, trade secrets or any other material covered by Idexcel's Confidential Information policy when engaged in blogging and social networking.
3. Employees shall not engage in any blogging and social networking that may harm or tarnish the image, reputation and/or goodwill of Idexcel and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Idexcel's Non-Discrimination and Anti-Harassment policy.
4. Employees may also not attribute personal statements, opinions or beliefs to Idexcel when engaged in Blogging and social networking. If an employee is expressing his or her beliefs and/or opinions in blogs or posts in social networking sites, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Idexcel Employees assume any and all risk associated with blogging and social networking.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Idexcel's trademarks, logos and any other Idexcel intellectual property may also not be used in connection with any blogging and social networking activity

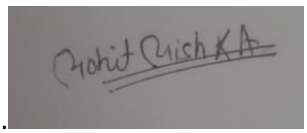
Acceptable Use of Assets Acknowledgement

I, **MOHI MISHRA** acknowledge I received a copy (digital or print) of Idexcel Acceptable Use of Assets. I acknowledge I read and understand all the information contained within the Idexcel and I agree to abide by Idexcel's policies, procedures, standards, and guidelines on acceptable use of assets.
I acknowledge that if I do have any questions regarding any information within Idexcel, it is my responsibility to address those issues with my supervisor for further clarification. I acknowledge that ignorance is not an excuse and I take full responsibility for my actions and the actions I fail to do. I acknowledge that failure on my part to practice due care and due diligence may also result in the termination of my employment for cause.

I agree to indemnify, defend and hold harmless Idexcel, its subsidiaries and affiliated companies, and each of its respective officers, directors, employees, shareholders and agents (each an "indemnified party" and, collectively, "indemnified parties") from and against any and all claims, damages, losses, liabilities, suits, actions, demands, proceedings (whether legal or administrative), and expenses (including, but not limited to, reasonable attorney's fees) threatened, asserted or filed by a third-party against any of the indemnified parties arising out of or relating to any and all gross negligence and/or misconduct on my part.



The terms of this acknowledgement shall survive any termination of employment.



Signature and Date

Human Resources Signature and Date 08-oct-2024