



ACCEPTABLE USE POLICY

Effective protection of company information and assets is a team effort involving the participation and support of every Duran HCP employee and affiliate who deals with information and/or information systems. It is the responsibility of every Permitted User to know these policies and to conduct their activities accordingly.

The purpose of this policy is to outline the acceptable use of the Company's systems. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues.

The Company provides Company property and resources, such as facsimile machines, copy machines, office supplies, computers, telephone access, voicemail, network, email (including instant messenger type service), and Internet access as well as other methods of information storage and communication to Permitted Users in order for Permitted Users to perform their work effectively. It is important for Permitted Users to be aware that access to these resources is a privilege, conditional upon adherence to this Policy.

Permitted Users. Employees and such other persons as the Company may specifically authorize.

No Expectation of Privacy. The computer and other electronic communications and information systems owned by the Company are provided for business purposes and are the property of the Company. Accordingly, the Company may access, review, monitor, copy, block and delete a Permitted User's communications for business reasons. Further, the Company may disclose Permitted User communications to third parties if appropriate. Thus, Permitted Users should not expect privacy in voicemail, email, or any communications on the network.

Inspection. Any property owned by the Company, including disks and storage media, desks, filing cabinets, or other work areas, as well as the articles contained therein, is subject to inspection by Company personnel at any time with or without notice or consent.

Passwords. Permitted Users are responsible for the security of their passwords and accounts. Permitted Users may not share their passwords, PINs, or passphrases with anyone, including other Permitted Users. Permitted Users may not gain access to other network accounts without prior management authorization. Permitted Users are strictly prohibited from accessing another Permitted User's Company accounts or communications without the latter's express permission.

Passwords protect communications from other Permitted Users and outside parties but are not intended to restrict Company access. The Company may access any files, voicemail, or email messages stored on or deleted from the Company's systems.



Permitted Activities. The Company provides network access for business purposes; however, the Company recognizes that, on occasion, a Permitted User may want to utilize the Internet or email for personal use. This use is permitted on a limited basis, so long as it is not illegal, does not violate our policies, interfere with productivity, disrupt morale, or undermine the Company's business objectives.

Permitted Users agree to use Company property and resources for the purpose of conducting Company business. Permitted Users must follow all applicable laws, regulations, and policies when utilizing these resources. Any communications through or with Company resources must be consistent with Company policies, standards, ethics, and values, should provide business benefit, and must be within one's work scope.

Prohibited Activities. Permitted Users agree to refrain from conducting prohibited activities. Without limiting any other part of this policy, Permitted Users may not use the voicemail system, a copy machine, a facsimile machine, or the Company network to send, receive, store, or display communications or files, including email attachments, that are illegal, disruptive, offensive to others, or harmful to morale. Such activities include, but are not limited to, activities that:

- Infringe any third party intellectual property right or right of publicity or privacy;
- Violate any law, statute, ordinance, or regulation, including anti-spamming laws;
- Are defamatory, threatening, harassing, insulting, abusive, or violent;
- Are sexually explicit, pornographic, indecent, profane, vulgar, or might be construed as harassing derogatory, disparaging, based, or discriminatory based on a person's age, sex, race, sexual orientation, disability, national origin, religion, or political belief; or,
- Are solicitations or advertisements for commercial ventures, religious or political causes, outside organizations, or other non-work related activities.

Third Party Materials. Permitted Users should not redistribute or copy third party materials without prior authorization by those third parties, unless they will not be violating the property rights of the owner of the material. Articles, photos, graphics, sound files, and other attachments are often the intellectual property of another party. Permitted Users should assume that anything they download from the Internet is protected by intellectual property laws, and the use or redistribution of those materials is governed by license from the content owners. Consult with the appropriate management or counsel for any questions regarding appropriate use of these materials.

Return of Company Property. Permitted Users are responsible for all property, materials, or written information issued to them or in their possession or control. Upon termination of employment or project assignment, or immediately upon request, Permitted Users must return to the Company all Company documents (and all copies thereof) and other Company property and materials in their possession or control. This includes, but is not limited to, Company files, notes, memoranda, correspondence, lists, drawings, records, plans and forecasts, financial information, personnel information, customer and customer prospect information, sales and marketing information, product development and pricing information, specifications, computer-recorded information, tangible property, credit cards, entry cards, identification badges and keys; and any materials of any kind which contain or embody any proprietary or confidential material of the Company (and all reproductions thereof) or any third party information. The Company may take all action deemed appropriate to recover or protect its property.



Unauthorized Transfer of Information. Transferring any proprietary or confidential Company information via any method to internal or external parties or hosts, without the express written permission of authorized personnel, is strictly forbidden.

Handling of Information.

- Any information that users consider vulnerable, sensitive, or that is deemed as such according to the Information Privacy Policy, must be encrypted when stored or transported.
- Because information contained on portable computers is especially vulnerable, special care should be exercised. If you are issued a laptop, protect it carefully.
- Sensitive information, as defined in the Information Privacy Policy, must not be left unattended and in plain sight (i.e. on a Permitted User's desktop).
- Information must not be left unattended on a screen or viewing device in plain sight. While unattended, the device must be secured by logging out, locking the computer, or using a password protected screen saver.

Email Retention. It is important for the Company's well being that email is used appropriately and that only current documents are maintained on the email system.

Prohibited Email Activities. The following activities are strictly forbidden:

- Sending unsolicited email messages, including 'junk mail' or other advertising material to individuals who did not specifically request such material (email spam);
- Sending any form of harassment via email, including, but not limited to, language, frequency, or size of messages;
- Unauthorized use or forging of email header information;
- Soliciting email for any other email address other than the poster's account, with the intent to harass or to collect replies;
- Creating or forwarding 'chain letters', 'Ponzi' or other pyramid schemes of any type;
- Using unsolicited email originating from within the Company's network on behalf of, or to advertise, any service hosted by the Company or connected via the Company's network;
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup SPAM);
- Accessing non-Company email accounts (i.e., POP3, IMAP) using Company provided mail client or management software; or,
- Automatically forwarding email from the Permitted User's work account to another email account.

Prohibited System and Network Activities. The following activities are strictly prohibited:

- Unauthorized copying, distribution, usage, or installation of copyrighted material that is not licensed to the Company, including but not limited to, software, music, and photos;
- Exporting software, technical information, encryption software, or technology in violation of international or regional export control laws. Appropriate management should be consulted prior to export of any material that is in question;



- Effecting security breaches or disruptions of network communication. Security breaches and disruptions include, but are not limited to, accessing data of which the Permitted User is not an intended recipient, logging into a server or account that the Permitted User is not expressly authorized to access, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes;
- Port scanning or security scanning;
- Circumventing user authentication or security of any host, network or account;
- Interfering with or denying service to any Permitted User;
- 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;
- Intentionally creating, using, or storing any viruses, Trojan horses, worms, time bombs, cancelbots, or other computer programming routines that are intended to damage, detrimentally interfere with, surreptitiously intercept, or expropriate any system, data or personal information;
- Using a host connected to a Company network that is not continually executing approved virus-scanning software with a current virus database;
- Implementing or connecting to any Company network via unauthorized wireless networks, equipment, or devices.
- Creating or using unauthorized access to Company networks, systems, or data including, but not limited to, modems and wireless devices;
- Congesting the network or interfering with the work of others, including the transmission or posting of messages that are intended or likely to result in the loss of the recipient's work or systems; or,
- Using the Company network to gain unauthorized access to third party resources.

Amendments to this Policy. This Policy supersedes all prior communications, oral or written, regarding use of Company property, resources, email, voicemail and the Internet. The Company may change, delete or add to the policies or practices described in the Acceptable Use Policy from time to time in its sole and absolute discretion with or without prior notice.

Acknowledged

Employee Signature

Date