NAVEX GLOBAL®
The Ethics and Compliance Experts

REFERENCE GUIDE

Acceptable Use Policy

GENERAL GUIDANCE NOTE:

This sample policy is not legal advice or a substitute for consultation with qualified legal counsel. Laws vary from country to country. Policies should have effective dates noted on the face of the policy and the company should retain an archive of earlier versions. This sample policy should not be implemented or executed except on the advice of counsel.

SAMPLE TEXT:

OVERVIEW

The Information Security Department ("**Infosec**") is committed to protecting Company's directors, officers, employees, contractors and the company from illegal or damaging actions by individuals. Infosec has issued this Acceptable Use Policy (this "**Policy**") in furtherance of this objective.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network resources and network accounts providing electronic mail, online browsing, and file transfer protocols (collectively, "**Computer Systems**"), are the property of Company. These systems are generally only to be used for business purposes in serving the interests of Company, and of Company's clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of everyone who handles Company information and information systems.

PURPOSE

The purpose of this Policy is to outline the acceptable use of Computer Systems at Company. These rules are in place to protect Company's information against loss or theft, unauthorized access, disclosure, copying, use, modification or destruction (each an "**Information Security Incident**"). Information Security Incidents can result in a broad range of negative consequences, including embarrassment, financial loss, non-compliance with standards and legislation and liability to third parties.

SCOPE

This Policy applies to the use of Company information and Computer Systems to conduct Company business or interact with internal networks and business systems, whether owned or leased by Company, the employee, or a third party.

All Individual Users are responsible for exercising good judgment regarding appropriate use of Company information and Computer Systems in accordance with Company policies and standards, and local laws and regulation.

This Policy applies to all directors, officers and employees of Company, as well as third-party contractors and agents of Company that have access to Company information or Computer Systems owned or leased by Company ("**Individual Users**" or "**you**").

POLICY

GENERAL USE AND OWNERSHIP

- Any Company proprietary information that is stored on electronic and computing devices, whether owned or leased by Company, the employee or a third party, remains the sole property of Company.
- You must ensure through legal or technical means that Company proprietary information is protected in accordance with this Policy.
- You are required to promptly report the theft, loss or unauthorized disclosure of Company proprietary information, or any other Information Security Incident.
- You may access, use or disclose Company proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
- You are responsible for exercising good judgment regarding the reasonableness of personal use of Computer Systems. Individual departments are responsible for creating guidelines concerning personal use of Computer Systems. In the absence of such policies, Individual Users should be guided by departmental policies on personal use, and if there is any uncertainty, Individual Users should consult their supervisor or manager.
- For security and network maintenance purposes, authorized Company personnel may monitor equipment, systems and network traffic per Infosec's Audit Policy.
- Company may audit Individual Users' use of Computer Systems as permitted by applicable law on a periodic basis to ensure compliance with this Policy.

SECURITY AND PROPRIETARY INFORMATION

- All mobile and computing devices that connect to Company's internal network must comply with the Minimum Access Policy.
- System-level and user-level passwords must comply with the Password Policy. Providing access to your passwords to another individual, either deliberately or through failure to secure its access, is prohibited.
- All mobile and computing devices must be secured with a password-protected screensaver that is automatically activated after 10 minutes of inactivity or less. You must lock the device's screen or log off when the device is unattended.
- If you use a Company email address to post to a newsgroup, forum or other group of third-party recipients, you should include a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of Company, unless the posting is made in the course of business duties.
- You must use extreme caution when opening e-mail attachments received from unknown senders or which are otherwise not expected and suspicious, since such attachments may contain viruses and other malicious code.

UNACCEPTABLE USE

The activities listed below are generally prohibited. Individual Users may be exempt from these restrictions during the course of their legitimate job responsibilities only with Infosec's written approval.

Under no circumstances is an Individual User permitted to engage in any activity that is illegal under local, state, provincial, federal or international law while using Company-owned resources or Computer Systems.

The lists below are not exhaustive and only provide examples of unacceptable use.

System and Network Activities

The following activities are strictly prohibited without exception:

- Violating the rights of any person or company under copyright, trade secret, patent or other intellectual property laws, such as by installing or distributing "pirated" or other software products that are not appropriately licensed for use by Company.
- Accessing Company information, Computer Systems or a user account for any purpose other than conducting Company business or as otherwise expressly permitted by Company policy or Infosec.
- Importing or exporting software, technical information, encryption software or technology in violation of applicable trade laws, including export control laws. The Legal Department should be consulted if you have any questions or concerns.
- Introducing malicious programs (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) to the Company network or server, or any other Computer System.
- Revealing your account password to, or allowing use of your account by third parties. For example, you may not share your account password with family or other household members when conducting work outside of the office.
- Using any Computer System to actively download or transmit material that violates sexual harassment or hostile workplace laws in the Individual User's local jurisdiction, or otherwise violates applicable laws or regulations.
- Making fraudulent or deceptive offers of products or services originating from any Company account.
- Making statements on Company's behalf about Company's representations, warranties, conditions or undertakings other than those pre-approved by the Company, unless the Legal Department's approval has been obtained.
- Causing or attempting to cause any security breaches, disruptions of network communications or Information Security Incidents. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and using forged routing information for malicious purposes.
- Port scanning or security scanning unless prior approval from Infosec has been obtained.
- Executing any form of network monitoring which will intercept data not intended for the Individual User's host except in accordance with Company policy.
- Circumventing user authentication protocols or the security of any host, network, account or other Company or third-party system.
- Introducing honeypots, honeynets, or similar technology on the Company network except in accordance with Company policy.
- Interfering with or disabling a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Company employees to parties outside Company.

Email and Communication Activities

Whenever Individual Users state or imply that they are affiliated with Company when emailing or communicating with third parties and such communications are not made in connection with Company business, they must clearly indicate that "the opinions expressed are my own and not necessarily those of the company".

In addition, the following activities are prohibited:

- Sending unsolicited email or other electronic messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- Engaging in any form of harassment via email, telephone or text messaging, whether through the content, frequency, or size of the messages.
- Forging email header information or otherwise including any misrepresentations or misleading information in email header information.
- Creating or forwarding chain letters or communications relating to Ponzi, pyramid or other fraudulent schemes of any type.
- Using unsolicited electronic messages originating from within Company's networks of other Internet/Intranet/Extranet service providers to advertise any service hosted by Company or connected via Company's network, unless specifically authorized in writing by the Legal Department.
- Posting the same or similar non-business-related messages to large numbers of Individual Users or other individuals.

Blogging and Social Media

Limited and occasional use of Company's Computer Systems to engage in blogging and social media activities ("blogging") is acceptable, provided that it is undertaken in a professional and responsible manner, complies with the Company's Social Media Policy, is not detrimental to Company's interests, and does not interfere with an Individual User's regular work duties. Blogging from Company's Computer Systems may be subject to monitoring.

In addition, the following activities are prohibited:

- Revealing any Company confidential or proprietary information, trade secrets or any other material covered by Company's Confidential Information Policy when blogging.
- Engaging in any blogging that may harm or tarnish the image, reputation and/or goodwill of Company and/or any of its employees.
- Making any discriminatory, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Company's Non-Discrimination and Anti-Harassment Policy.
- Attributing personal statements, opinions or beliefs to Company, or using Company's trademarks, logos or any other Company intellectual property without specific authorization from the Legal Department.

Individual Users assume any and all risks and responsibilities associated with using Company's Computer Systems to engage in blogging in a personal capacity.

POLICY COMPLIANCE

Infosec will monitor compliance with this Policy using various methods, such as business tool reports, internal and external audits, and any feedback provided to Infosec.

EXCEPTIONS

Any exception to this Policy must be approved by Infosec in advance.

NON-COMPLIANCE

All Individual Users are required to adhere to this Policy. Failure to comply may result in disciplinary action up to and including termination from employment for cause, termination of contract, and civil penalties and/or criminal sanctions, depending on the circumstances.

RELATED STANDARDS, POLICIES AND PROCESSES

- Audit Policy
- Social Media Policy
- Minimum Access Policy
- Password Policy
- Non-Discrimination and Anti-Harassment Policy
- Confidential Information Policy

RESPONSIBILITY FOR THIS POLICY

The [[BOARD OF DIRECTORS] OR [COMMITTEE] OR [POSITION]] has overall responsibility for the effective operation of this policy but has delegated day-to-day responsibility for overseeing its implementation to [POSITION]. All managers have a specific responsibility to operate within the boundaries of this policy, take effective steps so that all employees understand the standards of behavior expected of them, and to take action when behavior falls below its requirements. Managers will be given training in order that they may do so. Effective Date: [insert]

Backed by Baker & McKenzie
BAKER & MCKENZIE