NAVEX GLOBAL®
The Ethics and Compliance Experts

SAMPLE POLICY

Monitoring of Electronic Communications

DISCLAIMER

This sample policy is not legal advice or a substitute for consultation with knowledgeable and qualified legal counsel.

Baker McKenzie assumes no responsibility or liability for the contents of this generic policy, the only purpose of which is to illustrate some of the issues pertaining to the monitoring of employee electronic communications in the U.S.

The laws applicable to the monitoring of employee electronic communications may vary based on jurisdiction. Federal, state, and/or local law may apply depending on the location of the company, its operations, and its employees. While these laws are often similar, their differences can be material. The following sample policy does not account for the differences in applicable federal, state, and/or local law. This sample policy also does not account for changes in legislation, judicial and administrative precedent, or other developments and/or interpretations of applicable law.

Additionally, what are considered "best practices" for Company A may not be "best practices" for Company B. To be effective, a monitoring of electronic communications policy should not be a "cookie cutter" or a "one size fits all" policy. It should be tailored to the organization, and account for the company's specific workforce, operations, and industry.

THIS SAMPLE POLICY SHOULD NOT BE RELIED ON OR IMPLEMENTED AS A LEGALLY-COMPLIANT POLICY WITHOUT CONSULTATION FROM LEGAL COUNSEL.

MONITORING OF ELECTRONIC COMMUNICATIONS

All electronic communications, e-mail, voicemail, and other communications and information transmitted or received over Company systems are the sole property of the Company. The Company maintains the right to enter its systems, and to monitor, inspect, review, copy, delete, retain, and/or disclose any electronic communications or other information maintained on or transmitted over Company systems. The Company may do this at any time, for any purpose, with or without notification.

Employees should not assume that any electronic communications or other information transmitted or received over Company systems are private or confidential or that the Company or its designated representatives will not access and review the communications and information. Although certain applications may be password-protected, such protection is for the security of Company information, and should not be understood as providing employees with individual privacy. Individuals using Company equipment should have no expectation of privacy, and no expectation that any information stored on its systems—whether the information is contained on a computer hard drive, computer disks, personal folders or files, or in any other manner—will be private. Employees should not use Company e-mail, electronic communication systems, or other systems to send, receive or store messages not related to the Company's business that the employee wishes to keep private, personal or confidential.

The Company also may monitor and record Internet and other usage of its systems, as allowable by federal, state, and local laws. Employees should be aware that Company security systems are capable of recording (for each and every user) each World Wide Web site visit, each chat, newsgroup or e-mail message, each file transfer into and out of Company internal networks, and other usages of its systems.

Monitoring of e-mail, electronic communications, or other Company systems is not allowed by anyone other than persons specifically authorized to do so by Company management or as may be required by law.