Policy Statement:

The use of New England Law Boston's (NEL|B) automation systems, including computers, fax machines, and all forms of Internet/intranet access, is for NEL|B business and for authorized purposes only. Brief and occasional personal use of the electronic mail system, instant messaging or the Internet is not prohibited as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the NEL|B or otherwise violate this policy.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication must not be used to solicit or sell products or services that are unrelated to the NEL|B's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of NEL|B computers, networks, and internet access is a privilege granted by management and may be revoked at any time for any reason, or for inappropriate conduct carried out on such systems, including, but not limited to:

- Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate NEL|B purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of NEL|B files or other NEL|B data;
- Destroying, deleting, erasing, or concealing NEL|B files or other NEL|B data, or otherwise making such files or data unavailable or inaccessible to the NEL|B or to other authorized users of NEL|B systems;
- Misrepresenting oneself or NEL|B;
- Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the NEL|B's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Participating in partisan politics;
- Causing congestion, disruption, disablement, alteration, or impairment of NEL|B networks or systems;
- Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms", or private/personal/instant messaging;

- Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;
- Using recreational games; and/or
- Defeating or attempting to defeat security restrictions on NEL|B systems and applications.

Using NEL|B's automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material, defined as any visual, textual, or auditory entity, file, or data, is strictly prohibited. Such material violates the NEL|B's anti-harassment policies and is subject to disciplinary action. NEL|B's electronic mail system, internet access, and computer systems must not be used to harm others or to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of NEL|B resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. NEL|B will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual internet activities, email use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the NEL|B's automation systems is expressly forbidden.

If you violate these policies, you may be subject to disciplinary action, up to and including dismissal.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files; No Expectation of Privacy:

NEL|B owns the rights to all data and files in any computer, network, or other information system used at NEL|B and to all data and files sent or received using any NEL|B system or using NEL|B's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. NEL|B also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the internet and of computer equipment used to create, view, or access e-mail and internet content. Employees must be aware that the electronic mail messages sent and received using NEL|B equipment or NEL|B-provided internet access, including web-based messaging systems used with such systems or access, are not private and are subject to viewing, downloading, inspection, release, and archiving by NEL|B officials at all times. NEL|B has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with NEL|B policies and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate NEL|B official.

NEL|B has access to software that allows monitoring by authorized personnel and that creates and stores copies of any messages, files, or other information that is entered into, received by, sent, or viewed on such systems. Accordingly, employees should assume that whatever they do, type, enter, send, receive, and view on NEL|B electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and NEL|B use at any time. Further, employees who use NEL|B systems and internet access to send or receive files or other data that would otherwise be subject to any kind of confidentiality or disclosure privilege thereby waive whatever right they may have to assert such confidentiality or privilege from disclosure. Employees who wish to maintain their right to confidentiality or a disclosure privilege must send or receive such information using some means other than NEL|B systems or the NEL|B-provided internet access.

NEL|B has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail:

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and NEL|B rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of NEL|B policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others, unless such access is directly related to that employee's job duties. Employees found to have engaged in such activities will be subject to disciplinary action, up to and including dismissal.

Electronic Mail Tampering:

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet / Intranet Browser(s):

The internet is to be used to further NEL|B's mission, to provide effective service of the highest quality to NEL|B's community of faculty, staff, alumni and students, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the internet for professional activities and career development. The various modes of Internet / intranet access are NEL|B resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications.

Employees are individually liable for any and all damages incurred as a result of violating NEL|B security policy, copyright, and licensing agreements.

All NEL|B policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, NEL|B information dissemination, standards of conduct, misuse of NEL|B resources, anti-harassment, and information and data security.

Personal Electronic Equipment:

NEL|B prohibits the use or possession in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image- or voice-recording device without the express permission of NEL|B. Employees with such devices should leave them at home unless expressly permitted by NEL|B to do otherwise. This provision does not apply to designated NEL|B personnel who must use such devices in connection with their positions of employment.

Employees should not bring personal computers or data storage devices (such as floppy disks, CDs/DVDs, external hard drives, flash drives, iPods, or other data storage media) to the workplace or connect them to NEL|B electronic systems unless expressly permitted to do so by the NEL|B. Any employee bringing a personal computing device, data storage device, or image-recording device onto NEL|B premises thereby automatically gives permission to the NEL|B to inspect the personal computer, data storage device, or image-recording device at any time with personnel of the NEL|B's choosing and to analyze any files, other data, or data storage devices or media that may be within or connectable to the personal computer or image-recording device in question. Employees who do not wish such inspections to be done on their personal computers, data storage devices, or imaging devices should not bring such items to work at all.

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment. In addition, the employee may face both civil and criminal liability from the NEL|B, from law enforcement officials, or from individuals whose rights are harmed by the violation.