



# *Information Technology Security Policy*

*Buffalo and Erie County Public Library*

Approved per Resolution 2009-44 September 17, 2009

*Buffalo and Erie County Public Library*  
*Information Technology Security Policy*

*Table of Contents*

<b>I.</b>	<b>Purpose .....</b>	<b>Page 1</b>
<b>II.</b>	<b>Acceptable Use Policy .....</b>	<b>Page 1</b>
<b>III.</b>	<b>Audit Vulnerability Scan Policy .....</b>	<b>Page 7</b>
<b>IV.</b>	<b>Public and Staff PC Anti-Virus Policy.....</b>	<b>Page 8</b>
<b>V.</b>	<b>E-mail Use Policy .....</b>	<b>Page 9</b>
<b>VI.</b>	<b>Router Security Policy .....</b>	<b>Page 10</b>
<b>VII.</b>	<b>Virtual Private Network (VPN) Policy .....</b>	<b>Page 11</b>
<b>VIII.</b>	<b>Data Center Access Policy .....</b>	<b>Page 13</b>

## I. Purpose

The purpose of the Buffalo and Erie County Public Library (herein also referred to as the Library) *Information Technology Security Policy* is to maintain the Library's established rights and culture of openness, trust and integrity. The Information Technology Department is committed to protecting the Buffalo and Erie County Public Library's employees, users, partners and the Library from illegal or damaging actions by individuals, either knowingly or unknowingly.

## II. Acceptable Use Policy

### 1.0 Overview

Internet/Intranet-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 Buffalo and Erie County Public Library. These systems are to be used for business purposes in serving the interests of the Library, and of our patrons and vendors in the course of normal operations.

Information is a critical Library asset. It must be protected from unauthorized use, modification, destruction and disclosure.

Effective security is a team effort involving the participation and support of every Buffalo and Erie County Public Library employee and contractor who deals with information and/or information systems. It is the responsibility of every computer user to understand these guidelines and to conduct his or her activities accordingly.

### 2.0 Purpose

The purpose of this *Acceptable Use Policy* is to outline the acceptable use of staff computer equipment at the Buffalo and Erie County Public Library. These rules are in place to protect the employees, contractors and users of the Buffalo and Erie County Public Library. Inappropriate use exposes the Buffalo and Erie County Public Library to risks including virus attacks, compromise of network systems and services, compromise of bibliographic and financial information, compromise of personal information, and resultant legal issues.

### 3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and all other workers (including any third party affiliates) at the Buffalo and Erie County Public Library. This policy applies to all equipment that is owned or leased by Buffalo and Erie County Public Library.

### 4.0 Policy

#### 4.1 General Use and Ownership

Users must be aware that the data they create on the Library's systems remains the property of Buffalo and Erie County Public Library. Because of the need to protect the

Buffalo and Erie County Public Library's network, the Information Technology Department cannot guarantee the confidentiality of information stored on any network device belonging to the Buffalo and Erie County Public Library.

During work shifts, employee use of the Internet is for the sole purpose of conducting Library business.

For security and network maintenance purposes, authorized individuals within the Buffalo and Erie County Public Library may monitor equipment, systems and network traffic at any time.

The Buffalo and Erie County Public Library reserves the right to audit networks and systems on an ongoing basis to ensure the integrity, confidentiality and availability of information and resources.

## **4.2 Security and Proprietary Information**

### **4.2.1 Employee Responsibilities (General)**

The user interface for information contained on Internet/Intranet-related systems should be classified as either confidential or not confidential, as defined by Library's Circulation Policy, Erie County Employee Handbook, and any other Library-issued official memos which contain information on Library policy and procedure. Examples of confidential information include but are not limited to: Library employee or patron personal data, cardholder borrowing information, and internal financial or vendor information. Employees should take all necessary steps to prevent unauthorized access to this information.

Pursuant to New York Civil Practice Laws and Rules Section 4509, Library records that contain names or other personally identifying details of users, including but not limited to the circulation of Library materials, computer use, interlibrary loan transactions, reference queries, requests for photocopies of Library materials, title reserve requests, or the in-house use of Library materials, shall be confidential and shall not be disclosed except that such records may be disclosed for the proper operation of the Library and shall be disclosed upon request or consent of the user or pursuant to subpoena, court order or where otherwise required by statute.

Passwords must be kept secure and accounts should not be shared unless designated as a departmental or multi-user account. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly and must be changed when an authorized user is no longer employed by the Library.

All PCs, laptops and workstations dedicated to a single user with personal account access should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K and XP users) when the host will be unattended. Because information contained on portable computers is especially vulnerable, special care should be exercised. Laptops must be protected while traveling and should not be left unattended.

Postings by authorized employees from a Buffalo and Erie County Public Library e-mail address to newsgroups are permitted in the course of business duties, supporting a Library policy or professional issue. Employees are prohibited from submitting a personal comment or opinion.

All hosts used by the employee that are connected to the Library Internet/Intranet, whether owned by the employee or the Buffalo and Erie County Public Library, must be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, Trojan horses, or other harmful code.

#### **4.2.1 E-Commerce Information**

E-Commerce patron transaction data must be encrypted by the Buffalo and Erie County Public Library's e-Commerce server using industry -recognized SSL certificate with minimum RSA (1024) encryption.

E-Commerce software must be set to keep maximum of 8 outer digits of the patron's credit card number for reference.

Under no circumstances should a Library patron's credit card information be transmitted electronically, stored or filed in any hard copy format. Every effort must be made to insure that the patron's credit card information is not manually recorded at any time. In the extenuating circumstance that authorized personnel must manually record this information, the paper document must be immediately destroyed (shredded) by that employee at the conclusion of the transaction.

#### **4.3. Unacceptable Use**

Under no circumstances is an employee of the Buffalo and Erie County Public Library authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Library owned resources.

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of 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).

The list below is by no means exhaustive, but provides a framework for activities which fall into the category of unacceptable use.

#### 4.3.1 System and Network Activities

The following activities are strictly prohibited:

- 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 the Buffalo and Erie County Public Library.
- 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 Buffalo and Erie County Public Library or the end user does not have an active license or express permission is strictly prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate administrator should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Making fraudulent offers of products, items, or services originating from any Buffalo and Erie County Public Library user account or computer.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. 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.
- Port scanning or security scanning is expressly prohibited without prior notification to and the express permission of the Information Technology Department.
- 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.
- Circumventing user authentication or security of any host, network or account.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack attempting to make the computer resources unavailable to the intended users).

- 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.
- Providing information about, or lists of, Buffalo and Erie County Public Library employees, cardholders or computer users to parties outside the Library.

#### **4.3.2 E-mail and Communications Activities**

The following activities are strictly prohibited, with no exceptions:

- Revealing personal Buffalo & Erie County e-mail account passwords to others or allowing use of Library e-mail account by others. This includes, but is not limited to, family and other household members if a staff member has remote access.
- Using the Library's computing assets 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.
- Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).
- Any form of harassment via e-mail, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of e-mail header information.
- Solicitation of e-mail for any other e-mail address, other than that of 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.
- Posting non-Library-related messages to large numbers of Usenet newsgroups (newsgroup spam).

#### **4.4. Blogging**

Blogging by employees, pursuant to their positions, whether using Buffalo and Erie County Public Library's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Postings to any social networking sites are also subject to the terms and restrictions set forth in the Policy.

Authorized employees may use the Library's systems to engage in work-related blogging on staff PCs, provided that it is done in a professional and responsible manner, does not otherwise violate the Buffalo and Erie County Public Library security policy, is not detrimental to the Library's best interests, and does not interfere with an employee's

regular work duties. Blogging from the Buffalo and Erie County Public Library systems is also subject to monitoring.

Employees are prohibited from revealing any Buffalo and Erie County Public Library confidential or proprietary information.

Employees shall not engage in any blogging pursuant to their positions that may harm or tarnish the image, reputation and/or goodwill of Buffalo and Erie County Public Library and/or any of its employees.

Employees are prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the Buffalo and Erie County Public Library.

Employees may not attribute personal statements, opinions or beliefs to the Buffalo and Erie County Public Library when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Buffalo and Erie County Public Library.

Employees assume any and all risk associated with blogging.

Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, unless authorized conducting the normal course of business, the Buffalo and Erie County Public Library's logos and any other Library intellectual property may not be used in connection with any blogging activity.

### **5.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

### **6.0 Definitions**

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Social Networking	Refers typically to a web-based service with a focus of building on-line communities providing a variety of ways for users to interact.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

### III. Audit Vulnerability Scan Policy

#### 1.0 Purpose

The purpose of the *Audit Vulnerability Scan Policy* is to set forth standards for network security scanning performed by the Information Technology Department within the Buffalo and Erie County Public Library networks and shall utilize NESSUS software to perform electronic scans of networks and/or firewalls or on any system administered by the Library.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources;
- Investigate possible security incidents, ensure conformance to the Buffalo and Erie County Public Library security policies; and/or
- Monitor user or system activity where appropriate.

#### 2.0 Scope

This policy covers all computer and communication devices owned or operated by the Buffalo and Erie County Public Library. This policy also covers any computer and communications device present on the Buffalo and Erie County Public Library premises, but which may not be owned or operated by the Library.

#### 3.0 Policy

When requested, and for the purpose of performing an audit, members of the Information Technology Department are permitted to access the Buffalo and Erie County Public Library networks and/or firewalls to the extent necessary to allow performing the scans authorized in this agreement.

This access may include:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Buffalo and Erie County Public Library equipment or premises;
- Access to work areas (libraries, labs, offices, cubicles, storage areas, etc.); and/or
- Access to interactively monitor and log traffic on all Buffalo and Erie County Public Library networks.

**3.1 Service Degradation and/or Interruption.** Network performance and/or availability may be affected by the network scanning process. Information Technology Department employees must monitor the scanning process closely and if necessary terminate the process due to network performance degradation and/or failure.

**3.2 Point of Contact During the Scanning Period.** The Buffalo and Erie County Public Library shall identify, in writing, a person to be available if scanning team has questions regarding data discovered or requires assistance.

**3.3 Scanning period.** The Buffalo and Erie County Public Library and the Information Technology Department shall identify in writing the allowable dates for the scan to take place.

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**IV. Public and Staff PC Anti-Virus Policy**

**1.0 Purpose**

The purpose of the *Public and Staff PC Anti-Virus Policy* is to establish requirements which must be met by all computers connected to the Buffalo and Erie County Public Library networks ensuring effective virus detection and prevention.

**2.0 Scope**

This policy applies to all Buffalo and Erie County Public Library computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, tablet computers, handheld computers (PDAs), domain controllers, file/ftp/tftp/proxy/web servers and any other servers.

**3.0 Policy**

All Buffalo and Erie County Public Library PC-based computers must have the Library's system standard-supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Network Support Managers and Supervisors are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into Buffalo and Erie County Public Library's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the *Acceptable Use Policy*.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are excluded at the current time.

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## V. E-mail Use Policy

### 1.0 Purpose

The purpose of the *e-mail Use Policy* is to insure the integrity of the public image of the Buffalo and Erie County Public Library. When e-mail is transmitted from the Buffalo and Erie County Public Library the general public will tend to view that message as an official policy statement from the Library.

### 2.0 Scope

This policy covers appropriate use of any e-mail sent from a Buffalo and Erie County Public Library e-mail address and applies to all employees, contractors, and agents operating on behalf of the Buffalo and Erie County Public Library.

### 3.0 Policy

**3.1 Staff e-mail Accounts.** Library personal or departmental e-mail accounts are established for use by authorized staff to conduct Library business or Library-related communication.

**3.1 Prohibited Use.** The Buffalo and Erie County Public Library e-mail system shall not be used for the creation or distribution of any disruptive or offensive messages, including, but not limited to, inappropriate comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any Library employee should report the matter to their supervisor immediately.

### 3.2 Personal Use.

Using Library established accounts for personal e-mail is prohibited at all times. Using the Library's resources for any personal e-mail is unacceptable during work hours. Personal e-mail may be accessed during authorized breaks and lunch periods. Sending chain letters or joke e-mails from a Library e-mail account is prohibited. Virus or other malware warnings and mass mailings from a Library e-mail account must be approved by the Information Technology Department before sending. These restrictions also apply to the forwarding of mass e-mail received by a Library employee.

### 3.3 Monitoring

Buffalo and Erie County Public Library employees shall have no expectation of privacy in anything they store, send or receive on the Library's e-mail system. The Buffalo and Erie County Public Library may monitor messages without prior notice.

### 4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## 5.0 Definitions

Term	Definition
E-mail	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical e-mail clients include Eudora and Microsoft Outlook.
Forwarded e-mail	E-mail re-sent from an internal network to an outside point.
Chain e-mail or letter	E-mail sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to the Buffalo and Erie County Public Library or its patrons.
Virus warning.	E-mail containing warnings about virus or malware. The overwhelming majority of these e-mails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

## VI. Router Security Policy

### 1.0 Purpose

The purpose of the *Router Security Policy* is to describe a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at the Buffalo and Erie County Public Library.

### 2.0 Scope

All routers and switches connected to the Buffalo and Erie County Public Library production networks are affected.

### 3.0 Policy

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router.
2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.
3. Disallow the following:
  - a. IP directed broadcasts
  - b. Incoming packets at the router sourced with invalid addresses such as RFC1918 address
  - c. TCP small services
  - d. UDP small services

- e. All source routing
- f. All web services running on router
- 4. Use corporate standardized SNMP community strings.
- 5. Access rules are to be added as business needs arise.
- 6. Each router must have the following statement posted in clear view:

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS STRICTLY PROHIBITED. Explicit permission is required to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device.

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

**5.0 Definitions**

**Terms**

**Definitions**

Production Network The "production network" is the network used in the daily business of the Buffalo and Erie County Public Library. Any network connected to the Library's backbone, either directly or indirectly, which lacks an intervening firewall device. Any network whose impairment would result in direct loss of functionality to Library employees or impact their ability to do work.

**VII. Virtual Private Network (VPN) Policy**

**1.0 Purpose**

The purpose of the *Virtual Private Network (VPN) Policy* is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Buffalo and Erie County Public Library network.

**2.0 Scope**

This policy applies to all Buffalo and Erie County Public Library employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Library's network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

**3.0 Policy**

Approved Buffalo and Erie County Public Library employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet

Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Buffalo and Erie County Public Library internal networks.
2. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateway will be set up and managed by Buffalo and Erie County Public Library Information Technology Department.
6. All computers connected to the Buffalo and Erie County Public Library internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the Library standard, CA eTrust Treat Management - Antivirus Agent; this includes personal computers.
7. VPN users will be automatically disconnected from the Library's network after 30 minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Library-owned equipment must configure the equipment to comply with Buffalo and Erie County Public Library's VPN policy.
10. Only Buffalo and Erie County Public Library-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the Library's network, and as such are subject to the same rules and regulations that apply to Library's owned equipment, i.e., their machines must be configured to comply with Library's Security Policies.

#### **4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

#### **5.0 Definitions**

<b>Term</b>	<b>Definition</b>
IPSec Concentrator	A device in which VPN connections are terminated.

## VIII. Data Center Access Policy

### 1.0 Purpose

The purpose of the *Data Center Access Policy* is to define Buffalo and Erie County Public Library Data Center physical access policy and to ensure security measures are in place to protect the Data Center. The Data Center houses main servers, network devices and other critical infrastructure computing components that support all current Library services.

### 2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at the Buffalo and Erie County Public Library, including all personnel affiliated with third parties.

### 3.0 Policy

#### 3.1 Data Center Access Rules

Only authorized Library employees are allowed access to the Data Center. Each authorized employee is assigned unique access pass-code and each access is logged. The Library Security Office will only issue pass-codes to Security and Maintenance staff members who are responsible for regular monitoring or who may require emergency access, or staff authorized by the Information Technology Department Administrator. Authorized employees must be familiar with all Data Center policies, procedures and safety-related issues.

Access to anyone other than an authorized employee must be approved by the Information Technology Department Administrator or his designee. An authorized employee must remain with any visitor, vendor, etc. who has explicit permission to enter into the Data Center.

The secured area should only be accessed to meet a work-related requirement.

The door to the data center must remain closed at all times. During authorized entrance or exit from the data center, the door must not be kept open more than the time reasonably required.

Food, drink or other fluids are strictly prohibited in the secured areas.

### 4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.