

POLICY ON ELECTRONIC COMMUNICATIONS

Adopted by the Cabinet of Executives (June 15, 2001),
with additional sections adopted by the Planning Team (July 17, 2001)
and revisions adopted by the Cabinet of Executives (June 19, 2002; March 16, 2004;
November 2005; March 2007; December 2007)

1.5.1 STATEMENT OF POLICY

These policies (as outlined below) on electronic communication pertain to the churchwide organization of the Evangelical Lutheran Church in America (hereafter, ELCA), a Minnesota nonprofit corporation. These policies do not pertain to any other expressions of or entities related to this church.

The Evangelical Lutheran Church in America (ELCA) is committed to providing an environment that encourages the use of computers and electronic communications as essential tools to support the ELCA's mission and ministry. In utilizing the ELCA's computers and electronic communications systems, including, but not limited to, electronic mail and access to the Internet, it is important for all people using these systems (hereafter, Users) to be aware of the ELCA's policy regarding responsible use.

It is the responsibility of each User to ensure that this technology is used for proper business purposes and in a manner that (1) is responsible, professional, and legal; (2) does not compromise the confidentiality of proprietary or other sensitive information; (3) does not compromise the security of the ELCA's computer resources; and (4) is consistent with good stewardship and the mission and ministry of the ELCA.

1.5.2 ACQUISITION AND USE OF COMPUTER RESOURCES

1.5.2 A. Computer Resources. The term computer resources includes, but is not limited to, all hardware (including, but not limited to, personal computers, printers, scanners, servers, and hand-held personal digital assistants), software, computer systems, data, information, electronic mail, instant messages, Intranet and Internet services, and related systems.

1.5.2 B. Acquisition of Computer Resources. All computer resources for the ELCA shall be purchased by Information Technology (IT), or by the unit with the written approval of the executive for information technology. Requests for computer resources shall be submitted to Information Technology, with a Computer Equipment Request Form signed by the budget director of the unit requesting the purchase. The form is available on the ELCA Intranet. Requests will be approved only if the computer resources involved are necessary to carry out the mission and ministry of this church, as determined by the requesting unit executive, in consultation with the executive for information technology. All purchases in excess of \$5,000.00 must be approved by the Capital Budget Committee.

1.5.2 C. Ownership of Computer Resources. All computer resources provided to Users by or through the ELCA are assets of and owned by the ELCA. All User data, information, programs, electronic mail, graphic works, literary works, documentation, and other material created, received, sent, or stored using ELCA computer resources, whether or not designated as private or confidential, are assets of and owned by the ELCA, not the individual User.

1.5.2 D. Access. Whether and to what extent an individual is provided ELCA computer resources shall be determined by the executive of the unit in which the individual is employed or otherwise associated, in consultation with Information Technology. The extent to which an individual is provided access will be determined by the duties of the individual's position.

Requests for access to computer resources shall be forwarded to Information Technology using the User Security Profile Form. The form is available on the ELCA Intranet. Requests for access must be received at least three business days in advance of the need.

The ELCA may terminate or restrict an individual's access to ELCA computer resources at any time and for any reason. The decision to restrict or terminate an individual's access may be made by the individual's supervisor, unit executive, the executive for information technology, or the executive for administration. Access of a User will be terminated immediately at the end of the User's relationship with the ELCA. All e-mail subsequently sent to a former User's account will be undeliverable unless the User's former unit requests another individual (Proxy User) to receive e-mail sent to the account. Requests for a Proxy User will be granted where there is a business need to continue the former User's account. Proxy User requests should be submitted to Information Technology by e-mail. Upon the termination of a User's access, all computer resources in the possession of the User are to be returned to Information Technology.

Remote access through a Virtual Private Network (VPN) connection is available based on business need. The Remote Access request form, found under Information Technology in the forms section of the Intranet, must be completed and routed electronically. The form requires the approval of the executive for human resources and the executive for information technology in addition to the unit executive.

Information Technology annually will audit and update the User Access lists.

1.5.2 E. Systems Security. Information Technology is responsible for assessing the security risks and needs of ELCA computer resources along with developing and implementing appropriate security (Security Protocols). Without limiting the foregoing, the Security Protocols shall require Information Technology to track and record security incidents and address security issues related to: (1) access; (2) preservation, back-up, and recovery of data; (3) virus and other system attacks; and (4) the environmental, fire protection, redundancy, reliability, and controlled access requirements necessary to protect ELCA computer resources. Information Technology shall annually conduct a computer resource risk assessment and update the Security Protocols accordingly. A report of this annual assessment and any recommended updates to it shall be provided to the Cabinet of Executives. All Users are required to comply with the Security Protocols developed and implemented by Information Technology.

It is the responsibility of every User to protect ELCA computer resources from unauthorized access, modification, destruction, or disclosure. If a User is uncertain whether a particular use will jeopardize the security of any ELCA computer resource, the User must contact Information Technology before engaging in such use. Users must immediately advise the Information Technology Help Desk of any known or suspected security threat to any ELCA computer resource. Without limiting the foregoing, Users shall pay particular attention to the following:

- 1. Unattended Terminals.** An active terminal should not be left unattended for any extended period of time, for example, overnight or while the User is away from the office for several hours. For Users accessing computers by remote access, terminals must remain on.
- 2. Passwords.** Individual passwords for computers are confidential. Users are responsible for protecting their passwords and are restricted from giving them out to anyone other than an authorized ELCA employee. Users should change their network and application passwords when prompted. Each User is responsible for activity performed using the User's password. No User should attempt to obtain access to another User's electronic documents or computer resources without prior authorization. Only the User, the ELCA's officers, general counsel, executive for information technology, the User's supervisor, or unit executive can authorize access to the User's electronic documents or computer resources. If an unauthorized person gains access to a User's account, the User should contact Information Technology immediately.

Users of ELCA laptop computers are required to use a power-on password in order to access their laptop. The power-on password is assigned by Information Technology and cannot be changed. The User also is forbidden from disabling or changing several other passwords, such as the Windows Administration, MS Windows, or the BIOS (i.e., the built-in software that determines what a computer can do) passwords required by Information Technology to manage and troubleshoot the laptops. Users also will authenticate to the network using their passwords. All unattended laptops must be secured.

- 3. Virus Protection.** All files originating from a source outside the ELCA, including files obtained over the Internet, must be checked for possible computer viruses before being downloaded onto an ELCA computer. The virus-checking software on each ELCA computer ordinarily will perform this check automatically. If the virus checking software detects a virus, Users will receive a virus warning message. When this message occurs, Users are prohibited from using their computers until given permission to do so by an Information Technology technician. If a User suspects that a file may pose a virus risk, the User should contact Information Technology before downloading the file.
- 4. External Network Connections.** Only authorized personnel working at sites administered by the churchwide organization may establish Internet or other external network connections. Because other connections may cause unauthorized access to the ELCA's systems and information, they are strictly prohibited. Prohibited connections include, but are not limited to, the establishment of hosts with public modem dial-ins, World Wide Web Home Pages, and File Transfer Protocol (FTP).

5. **Data Backup.** All Users should save important data and information to their designated location on the ELCA network to assure it is protected, preserved, and recoverable in the event of a computer resource failure. The network is backed up to assist in data recovery in the event of a computer resource failure. Other locations to which data and information may be saved, such as PC hard drives, are not. Users who save data and information to locations other than their designated one do so at their own risk. Users without access to a network server, including deployed staff, should contact Information Technology for assistance with data backup.

Laptop Users are responsible for ensuring that their laptop backup is current. Procedures for laptop backup as determined by Information Technology must be followed. The procedure is found under Helpful Hints, Information Technology.

6. **Data and File Security.** The ELCA owns all rights to all data that originates on its systems. This includes but is not limited to data in database format, e-mail, and word processing and spreadsheet documents. ELCA staff member assigned as the primary User of any business-related computer system or software is responsible for the integrity of the data within his or her systems. The appropriate management team in each unit authorizes access to the data and assumes risk if the data is left unprotected.

The Cabinet of Executives is responsible for setting policies related to the security of the information systems of the ELCA. A risk assessment will be conducted regularly in consultation with the internal auditor to ensure that appropriate measures are implemented to provide for the availability and security of critical ELCA data.

Users may not install or use encryption software on any of the ELCA churchwide computers without first obtaining written permission from Information Technology.

Unit staff members are responsible for the security, distribution, and proper disposal of reports that are directed to unit printers as well as all electronic information. Proper disposal should ensure the confidentiality of the data contained in reports.

Laptops will be configured with a power-on password that shall not be changed. Users also will authenticate to the network using their network password. All unattended laptops must be secured.

Data will be classified as confidential, restricted, or public, as determined by the originator in consultation with Information Technology and the internal auditor. Users working on confidential or restricted data are responsible for the proper handling of this data. Further guidelines on this matter are under development and will be available on the Intranet when approved.

7. **Business Continuity Planning.** The BCP Recovery Team is responsible for ensuring that adequate planning occurs for business continuity at the Lutheran Center. Each churchwide unit is responsible for developing a continuity plan. The Information Technology section shall maintain a Business Recovery Plan for network services.

1.5.2 F. No Privacy. Users do not have a personal privacy right in any matter created, received, sent, or stored on ELCA computer resources, telephone, or third-party resources used for work-related matters, whether or not the matter is designated as private or

confidential. The ELCA reserves the right, at any time and without prior notice, to monitor its computer resources and to read, listen to, and copy all files or data contained on any computer resource including, but not limited to, e-mail messages, Internet access records, voicemail messages, Internet discussion groups, and personal file directories. The ELCA reserves the right to access all computer resources for the purpose of supporting the mission and ministry of this church, assuring compliance with statutory requirements and internal policies supporting the performance of internal investigations, and assisting with the management of the ELCA's information systems.

1.5.2 G. Software License Restrictions and Trademark and Copyright

Laws. Most proprietary software licenses have legal restrictions prohibiting unauthorized use and copying. Software may not be loaded, downloaded, or received on any ELCA computer, including software available on the Internet, unless it is approved in advance by the executive for information technology. Only personnel authorized by the executive for information technology may: (1) load, download, or receive software onto any ELCA computer resource; (2) connect any hardware or other equipment to any ELCA computer resource; or (3) move or change any ELCA computer equipment. Information Technology shall maintain a file of all software licenses. If an individual is authorized to load, download, or receive software by Information Technology, that individual shall be responsible for forwarding the software license to Information Technology. Users never should install programs or updates unless directed or approved by Information Technology to do so.

Information posted, viewed, or downloaded from the Internet may be protected by copyright or piracy laws. Reproduction of protected information is permitted only if such reproduction is (1) permissible under applicable trademark, copyright, and piracy laws or (2) based on express permission given by the trademark or copyright owner, which must be filed in the unit using the information or material. It is each User's responsibility to comply with applicable trademark, copyright, and piracy restrictions. If Users have any questions about this matter, they should contact the ELCA legal staff before downloading, copying, transmitting, or reproducing any graphic works, data, software, or other information or material.

1.5.2 H. Prohibited Uses. It is the responsibility of each User to use ELCA computer resources in a manner consistent with the mission, ministry, and good stewardship of this church. Without limiting the foregoing, Users shall not use ELCA computer resources in any way that:

1. violates any law, statute, regulation, or ordinance;
2. violates any policy or procedure of the ELCA;
3. jeopardizes the security of any ELCA computer resource;
4. jeopardizes the tax-exempt status of the ELCA, any synod or congregation of this church, or any affiliate listed under the ELCA Group Ruling for federal income tax exemption, including transmission of political or partisan campaign materials;
5. violates the legal rights of any person or entity;
6. creates unauthorized contractual liability for the ELCA;
7. gives the impression a User is representing, giving opinions, making statements or commitments on behalf of the ELCA, unless authorized to do so by the ELCA;
8. results in the transmission or receipt of immoral, obscene, pornographic, discriminatory, harassing, or defamatory material;
9. interferes with the use of ELCA computer resources or the computer resources of another person or entity;

10. involves personal financial gain, lotteries, gambling, or raffles;
11. is inconsistent with norms of professional and business conduct; or
12. reflects adversely on the ELCA.

If Users have questions or concerns about the use or restriction on use of a computer resource, they should discuss the matter with their supervisor, their unit executive, or the executive for information technology.

1.5.3 RESPONSIBLE USE OF THE INTERNET

1.5.3 A. The Internet is for work-related purposes. The ELCA’s connection to the Internet is principally for work-related purposes through e-mail and access to the Worldwide Web. Unauthorized use of the Internet is prohibited. Unauthorized use includes, but is not limited to, any of the prohibited uses above.

1.5.3 B. Participation in work-related Internet discussion groups (which include, but are not limited to, chat rooms, blogs, or social networking sites) is permitted with certain restrictions. Users are responsible for ensuring that all information they share in work-related Internet discussion groups, chat rooms, blogs, or social networking sites is accurate and that any personal opinions they express are clearly identified as “personal” and not the opinion of the ELCA. Such participation is allowed to the extent that it (1) does not reflect adversely on the ELCA; (2) does not deter from regular work assignments; and (3) is consistent with all the ELCA’s standards and policies, including 1.5.2H. See related Guidelines.

1.5.3 C. Take precautions when providing information. A User should never provide confidential, proprietary, or restricted information about the ELCA, its employees, synods, congregations, members, or vendors without proper prior written consent by the ELCA.

1.5.3 D. Take precautions when obtaining information. Information obtained from the Internet is not subject to quality controls and should be verified by an independent source before being relied upon.

1.5.3 E. The ELCA may monitor Internet usage. The ELCA reserves the right to monitor at its discretion in the ordinary course of business Internet usage.

1.5.3 F. Users should be aware of the Web Site Terms of Use and Web Site Privacy Policy. The ELCA Web Site Terms of Use (www.elca.org/termsfuse.html) provide important information on use of the ELCA Web site contents, posting and linking policies, and other information for third-party users. The ELCA Web Site Privacy Policy (www.elca.org/privacypolicy.html) describes practices with regard to personal data collected through the Web site.

1.5.4 RESPONSIBLE USE OF E-MAIL

1.5.4 A. E-mail defined. For purposes of these policies, the term “e-mail” is any electronic message sent in any form from one computer to another including, but not

limited to, (1) electronic mail; (2) electronic messages sent to chat rooms; (3) bulletin boards; (4) list servers; and (5) instant messaging.

1.5.4 B. E-mail is for business purposes. The purpose of e-mail is to facilitate business communications among ELCA Users and to enable ELCA Users to carry out the duties of their positions.

1.5.4 C. E-mail correspondence is the property of the ELCA. All e-mail correspondence, whether or not related to personal or confidential matters, is the property of the ELCA. The ELCA reserves the right, at its discretion in the ordinary course of business, to monitor its e-mail system, including a User's mailbox. The existence of "passwords" and "message delete" functions does not restrict or eliminate the ELCA's ability or right to access electronic communications. In certain situations the ELCA may be compelled to access and disclose messages sent over its e-mail system.

1.5.4 D. Offensive, demeaning, harassing, defamatory, illegal, or disruptive e-mail is prohibited. E-mail should conform to the same standards of propriety and respect as any other verbal or written business communication. Sending or forwarding offensive, demeaning, harassing, defamatory, illegal, or disruptive messages is prohibited. This includes, but is not limited to, messages that are inconsistent with the ELCA's "Conduct in the Work Place" policies. Users who become aware of or receive prohibited e-mail should notify the ELCA's executive for human resources. Inappropriate use of e-mail may be grounds for discipline, up to and including termination of employment.

1.5.4 E. Users are responsible for eliminating inappropriate e-mail. When receiving e-mail from outside sources, Users have the responsibility of immediately deleting all e-mail that falls below the ELCA's standards as articulated above, including all pornographic, obscene, offensive, partisan political, and sexually explicit communications. Users also have the responsibility of ensuring that the prohibited e-mail is not seen by others. If the sender is a person known to the User, the User has the responsibility of informing the senders of the e-mail that such communications are prohibited from ELCA premises and equipment and should not be sent in the future.

1.5.4 F. E-mail is available remotely using GroupWise Remote or GroupWise Web Access. GroupWise Remote must be installed on ELCA computers by a technician from Information Technology. GroupWise Web Access can be accessed through the Internet at <https://webmail.elca.org/gw>. An Internet connection is required for the use of both methods.

1.5.4 G. Sending broadcast messages.

- 1. Internal Broadcast Messages.** Broadcast messages to the ELCA group may be sent with prior approval of the User's unit executive.
- 2. External Broadcast Messages.** Only the executive for administration or the ELCA secretary can authorize a User or unit to send other unsolicited broadcast messages including, but not limited to, broadcast messages to any grouping of synods, regions, congregations, and rostered persons.

1.5.4 H. Creation and Operation of List Servers, Bulletin Boards, and Chat Rooms. A User may establish a list service, bulletin board, or chat room using ELCA computer resources with the permission of the User's unit executive and Information Technology.

The User shall be responsible for ensuring that the list server, bulletin board, or chat room is operated as specified by Information Technology. The ELCA may terminate—at any time, for any reason, and without notice—the operation of a list server, bulletin board, or chat room operated using ELCA computer resources.

1.5.4 I. Deletion, Retrieval and Permanent Destruction of E-mail. Once e-mail is 41 days old, it is deleted automatically unless it has been archived by the User. Deleted e-mail will not be recovered for Users. In some cases, e-mail may have been backed up to an electronic tape by Information Technology. Backups are erased annually. Retrieval of an e-mail from backup will be authorized by the executive for information technology only when legally required.

1.5.4 J. Spam Filter. The ELCA provides a spam filter service for staff e-mails. It is the responsibility of each employee to review the quarantined report and to release any items that may be legitimate e-mails.

1.5.5 WEB-SITE DEVELOPMENT, CONTENT, AND SECURITY

The ELCA churchwide organization has developed Web-site development protocols (www.elca.org/communication/webrequirements.html). These protocols are designed to ensure all ELCA unit Web sites are high quality, secure, legal, and technically compatible with the ELCA churchwide organization Web site. All ELCA unit Web sites are required to be developed in compliance with these protocols. This applies even if third-party providers are hosting, developing, designing, or assisting in unit Web sites.

1.5.5 A. Development of New Sites or Redesign of Existing Sites. When new unit Web sites are designed or existing sites are substantially redesigned, the ELCA Web Manager must be consulted before work begins. The Web Manager will review the plans with the unit to identify items that must be checked with the protocols for quality and legal compliance and will consult Information Technology as appropriate. Users must complete the ELCA Web Development Checklist (Checklist), available online (www.elca.org/communication/webrequirements.html). Upon completion of the unit site, the unit must submit the completed Checklist, which will assure that all qualitative and legal requirements have been met. Final permission for posting will be granted by the Web Manager after the completed Checklist has been received and reviewed.

1.5.5 B. Collecting Information from Web-site Visitors. Soliciting personal information from visitors to a Web site, especially children, can raise a number of legal issues. Accordingly, the Web Manager and ELCA legal staff must approve any such solicitation, including surveys, before they can be placed on unit Web sites. In addition, surveys must be approved by Research and Evaluation.

1.5.5 C. Online Financial Transactions. Online financial transactions, including credit card transactions, raise a number of legal and security issues. Accordingly, all Web sites involving the exchange of financial information or financial transactions may be posted only after completion of the forms available from the Office of the Treasurer related to online financial transactions.

1.5.5 D. Independent Contractor Web-site Development Contracts. Units may desire to use independent contractors to develop part or all of a particular Web site. The creation of a Web site involves a myriad of legal, technical, artistic, and content issues and concerns. In order to protect the ELCA and ensure that all churchwide organization Web sites are consistent with the ELCA electronic communications policy and protocols, a standard Web-site development contract (Development Contract) has been developed. If a unit wants to contract with an independent contractor, it must consult with the Web Manager. The contract must then be approved by the Internet Services Committee.

1.5.5 E. Approval of Content for Units Involved in State or Federally Regulated Activities. Some units are involved in activities subject to state or federal regulations. It is the responsibility of the unit executive to ensure that all content placed on any Web site operated by the unit is in compliance with any applicable state or federal regulation. If a unit executive has any questions, the unit executive should contact the legal staff before posting the page.

1.5.5 F. Questions about Developing a Web site. All questions about developing Web sites should be directed to the Web Manager in Communication Services.

1.5.6 VOICEMAIL

1. Voicemail and the data stored on it are and remain at all times the property of the ELCA. As such, all voicemail messages created, sent, and received are and remain the property of the ELCA.
2. The company has the right to retrieve and listen to any message composed, sent, or received.
3. Messages should be limited to the conduct of the company's business. Voicemail is intended for business purposes only, and personal use is to be kept to a minimum. Using the company voicemail system to conduct home-based side businesses, Internet-based businesses, or any other part-time business is strictly prohibited.
4. Voicemail will be consistent with all ELCA standards and policies, including 1.5.2H.
5. All reasonable and necessary means of preserving voicemail contents for seven days are taken.

1.5.7 PROCEDURE FOR RECEIVING GROUPWISE EMAIL USING A PORTABLE DEVICE

1.5.7a Devices that are supported. The only phone/PDA device that the ELCA purchases at this time is the Sony TREO. Prior approval from the unit executive director/executive and the Executive for Administration is required for this device to be purchased by the ELCA. Other than the approved device listed above, churchwide units of the Evangelical Lutheran Church in America may not purchase or allow users to expense the purchase of PDA devices.

If a staff member purchases a PDA and desires to synchronize it with the GroupWise system, the PDA must be on the approved device list. *This list is found on the ELCA Intranet under "Approved PDA's".* Information Technology will provide the software required to sync the device with the GroupWise system at no additional charge to the unit. The only approved software for syncing such devices is the GroupWise Mobile Server software. Only Information Technology staff members may install such software.

1.5.7b Support provided by the Information Technology staff. Support is based on the following categories:

1. Device purchased by the ELCA and approved by the Executive for Administration
 - The ELCA will provide support of PDA devices when being used to perform ELCA related work.
2. Device purchased with staff members own funds and has their own data / voice plan NOT paid for by the ELCA. See the policy for reimbursement of cell phone usage in the Travel Policy E.2. The ELCA will provide support of PDA devices when being used to perform ELCA related work, but will not be able to provide assistance in the following cases:
 - The device malfunctions because of a hardware failure or user misuse.
 - The device is new and needs to be configured for the first time.
 - The device is damaged in any way by the user.
 - Software other than the GroupWise Mobile Server is used.

1.5.8 REMOTE ACCESS POLICY

1.5.8 A. Purpose The purpose of this policy is to establish standards for a consistent process for Remote Access for all users being employees, interns, contractors and agents of the churchwide office of the ELCA to securely connect to the Churchwide Office (CWO) network and to minimize the potential exposure to the CWO of the ELCA from loss or damages which may result from unauthorized use of its computer systems and/or resources. Damages may include the loss or misuse of sensitive or ELCA confidential data, intellectual property damage to public image, damage to critical internal systems, etc. These losses could represent a liability for the ELCA.

1.5.8 B. Scope This procedure applies to all users including employees, interns, contractors, authorized third parties and agents with an ELCA-owned or personally-owned computer or workstation used to connect to the CWO network. This policy applies to remote access connections used to do work on behalf of the ELCA, including reading or sending e-mail and viewing intranet web resources.

1.5.8 C. Remote Access Request Remote Access will be made available on a business need basis. This access will be strictly controlled, using appropriate password authentication and will be made available to an employee or agent on a business need basis. All persons requesting Remote Access must have a signed Electronic Communication Policy form on record with Human Resources. This person is required to complete a Request for Remote Access form located on the Intranet under IT forms. This form must be approved electronically by the requestor's department manager and sent to Information Technology for final approval by the appropriate people. The request must be submitted at least three business days prior to the need for access.

1. Remote Access for employees/agents will be allowed through the use of Equipment owned by or leased to the ELCA or through the use of the requestors own computer system.
 1. The ELCA is not responsible for the purchase, setup, maintenance or support of any Equipment which is not owned by or leased to the ELCA.
 2. Further, any Equipment, software and/or Public Network service charges incurred for Remote Access will be the responsibility of the employee, regardless of equipment ownership unless otherwise approved by the Executive for Administration and the Treasurer.
 3. The ELCA will not be responsible for any problems or loss that may be caused by installation of software on user's computer or by remote access by user.
 4. All users understand that the ELCA Terms of Use apply to Remote Access use.
 5. Only one employee computer will be set up for Remote Access.
2. Consultants and vendors may be granted Remote Access to ELCA Networks provided they have a contract with the ELCA which clearly defines the type of Remote Access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed by the Executive of Information Technology and approved by the Executive of Human Resources before Remote Access will be permitted. All such agent authorizations will have set time window and termination date, typically not to exceed one year. It will be the responsibility of the user to renew if a grant beyond the initially authorized time is needed.
3. It is the responsibility of those granted Remote Access to ensure the connection to the ELCA network is not used by non-employees or unauthorized persons or agents to gain access to ELCA information, data, or system resources. Remote Access employees/agents are expected to take every reasonable measure to protect the assets of the ELCA.
4. A Remote Access employee/agent is responsible for adherence to all ELCA Policies and Procedures. Users bear responsibility for the consequences should Remote Access be misused.

1.5.8 D. Compliance

1. Logs will be maintained by Information Technology of activities performed by Remote Access employees/Agents while connected to the ELCA Network.
2. When employment ends, Human Resource will notify Information Technology to enable them to terminate access.
3. For agents and third party users, Information Technology will maintain and act on calendar log of authorized use termination dates.

4. When using Public Network Services, Remote Access employees/agents are required to disconnect their ELCA network connectivity whenever their computer systems are idle for greater than 30 minutes.

1.5.9 PROCEDURE FOR PROVIDING TECHNOLOGY EQUIPMENT AND SUPPORT TO DEPLOYED STAFF

1.5.9 A Governing policies. The following statements from the Electronic Communication Policy (November, 2005) will provide the guiding principle for this policy:

1.5.2 B. Acquisition of Computer Resources. All computer resources for the ELCA shall be purchased by Information Technology (IT), or with the written approval of the executive for IT by the unit.

1.5.2 C. Ownership of Computer Resources. All computer resources provided to Users by or through the ELCA are assets of and owned by the ELCA. All User data, information, programs, electronic mail, graphic works, literary works, documentation, and other material created, received, sent, or stored using ELCA computer resources, whether or not designated as private or confidential, are assets of and owned by the ELCA, not the individual User.

1.5.9 B. Deployed Staff in a home or non-shared office

Equipment: Desktop computers and laptops will be replaced based on the churchwide office rotation schedule. Other technology purchases such as printers, software, etc must be purchased through the IT administrative assistant for purchasing. The items will be charged to the ordering unit. Equipment purchased directly by a staff member in this category will not be reimbursed unless prior permission is given by IT. (Call Janet Tortoriello at 2463)

Support: The churchwide office helpdesk will provide support for GroupWise, VPN, Formatta and hardware problems that can be addressed remotely. The deployed staff member in consultation with a helpdesk technician will be responsible for contacting and working with a local technical support company when needed. This support will be paid for by the unit.

Ownership of assets: The ELCA is the owner of any computer related asset.

1.5.9 C. Deployed Staff on another network

Equipment: Desktop computers and laptops will be replaced based on the churchwide office rotation schedule or the schedule of the organization providing the network. However, any equipment purchased on behalf of the ELCA by another partner must be pre-approved by the churchwide IT section. An appropriate decision will be made only after a conversation with a technical representative of the partner. Other technology purchases such as printers, software, etc must be purchased through the IT administrative assistant for purchasing. The items will be charged to the ordering unit. Equipment purchased directly by a staff member in this category will not be reimbursed unless prior permission is given by his/her unit and IT. (Call Janet Tortoriello at 2463)

Support: The churchwide office helpdesk will provide support for GroupWise, Formatta and VPN use. The network staff of the partner should be contacted for other support.

Ownership of assets: When the equipment is purchased by the partner the ELCA will reimburse the partner and the asset will belong to the ELCA.

1.5.9 D. Shared staff

Equipment: If a shared staff person's main office is at the location of the sharing partner, that partner should purchase computer equipment. The equipment will be the asset of the partner. The ELCA portion of the expense of the equipment will be the responsibility of the unit the person works with. If a shared staff person's main office is at the churchwide office, the unit the person works with will purchase the equipment through IT and invoice the sharing organization for its percent of the cost. The contract with the employee and partner should state the arrangement. If the person is shared by two or more units at the churchwide office with the churchwide office as the sole employer, the equipment will be expensed to the shared pool.

Support: Support will be provided by the staff at the primary location of the person. If support is needed on software provided by the ELCA and that is required for the responsibilities of the person, call the helpdesk at extension 2472 for support.

Ownership of assets: The organization purchasing the equipment will hold that asset.

1.5.9 E. Person Acting as an agent of the churchwide organization of the ELCA (example: FO fundraiser, consultant, etc.)

Equipment: The contract with the agent must include the arrangement for computer equipment. Equipment for an agent will not be purchased through the ELCA pool unless authorized by the Office of the Treasurer.

Support: The agent may receive assistance with software such as Raiser's Edge that is required for the working relationship.

Ownership of assets: The purchasing entity will hold the asset.

1.5.9 F. Return of equipment. *At the end of the lifecycle of any equipment or upon separation from employment, the deployed staff person must contact his/her unit representative for information on how to either return the equipment or donate it to a partner organization. This decision will be based on the age of the equipment and the cost of returning it to the churchwide office.*

1.5.9 G. Required security features Laptops will be configured with a power-on password that shall not be changed. The user will also authenticate to the network using his/her network password. All laptops must be secured with a lock when located in a work area. Laptops should never be left in the passenger area of a parked car. Secure important equipment or papers in a locked trunk or keep them with you.

Laptop users are responsible for assuring that their laptop backup is current.

The following software that protects the hardware and software assets are required: Symantic Antivirus, ELCA Information Technology approved backup client, Cisco VPN client. This software is installed by the ELCA and may not be disabled.

1.5.9 H. Access options

1. Remote access through a Virtual Private Network (VPN) connection is available based on business need. The Remote Access request form found under Links You Need/Forms/IT in the forms section of the Intranet must be completed and routed electronically. The form requires the approval of the Executive for Human Resources, the Executive for Information Technology in addition to the unit executive director or executive.

2. E-mail is available remotely using GroupWise Remote or GroupWise Web Access. GroupWise Remote must be installed by a technician from Information Technology. GroupWise Web Access can be accessed through the Internet at <https://webmail.elca.org/gw> . An Internet connection is required for the use of both methods.

1.5.9 I. Employee Training Opportunities. Employees are responsible for maintaining skills using the software required for their work. The following tools are available for your use:

1. Posted documentation and training aids can be found by clicking on Information Technology under Helpful Hints.
2. VPN: Deployed staff will be trained by churchwide staff in the use of the VPN client. Call the helpdesk if you experience problems.
3. The following systems have documentation or training available on the Intranet:

Time and Attendance
Use of forms on the Intranet
GroupWise
Software that protects the asset such as antivirus, malware and firewall software
Raiser's Edge
MicroSoft Office (Word, Excel, PowerPoint)

Units are encouraged to offer training as a part of unit meetings when deployed staff are present. The ELCA IT trainer is available to work with units to meet their specific needs.

1.5.9 J. Unit specific procedures. It is strongly recommended that units require the use of the GroupWise email and the GroupWise calendar to enable more efficient collaboration between units, deployed and Chicago based staff and the technical staff. Use your elca.org email address when representing the ELCA to your constituents.

1.5.10 COMPLIANCE REQUIRED

All Users must comply with the ELCA's Electronic Communications Policy. Violation of any of the terms of this policy may result in discipline, up to and including termination of employment.

Date: December 11, 2007