# 

# **OUR VISION AND MISSION**

# It is our vision to expand our church so that it continues to be a church of greater influence and impact to our community and the world. Our church is a church that will grow in representing our Lord Jesus Christ as He is worthy to be represented, presenting the good news of salvation, in season and out of season, to all who are not saved, so that they receive deliverance from all oppression by ensuring his eternal life and a better life on earth. We are a body of believers who will continue to alleviate suffering to all who are oppressed with spiritual, emotional, physical or family needs, through the anointing of the Holy Spirit, the gifts He has given us and the resources He entrusts to us. We will continue to develop believers through: The Biblical Training Seminar, meetings, conferences, and to raise a more formal educational body within the church, where pastors, missionaries and God's workers will be trained, so that each believer can perform in the service of God, through serving others. We will strengthen our commitment to the generations that come after us, our children and our youth, intensifying our work with them by preparing them to be a powerful generation in the midst of a world full of challenges, needs and evil. We will continue to develop our local mission through going to communities in NJ where the Lord sends us to open campuses (headquarters) assigning a pastor to each one and keeping us unified in vision and work using technology. We will continue to expand our missionary program by opening new works in other nations, and covering others already established, thus expanding the scope of the mission that the Lord has entrusted to us. "and the people will run because of the vision ..."

# 

# **1.** **Overview**

InfoSec intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to CBNJ’s established culture of openness, trust and integrity. Infosec is committed to protecting CBNJ's volunteers, partners and the church from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-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 CBNJ. These systems are to be used for church purposes in serving the interests of brothers and sisters in the course of normal operations.

Effective security is a team effort involving the participation and support of every CBNJ volunteer and employee who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

# **2.** **Purpose**

The purpose of this policy is to outline the acceptable use of computer equipment at CBNJ. These rules are in place to protect CBNJ property. Inappropriate use exposes CBNJ to risks including virus attacks, compromise of network systems and services, and legal issues.

# **3.** **Scope**

This policy applies to the use of information, electronic and computing devices, and network resources to conduct CBNJ business or interact with internal networks and business systems, whether owned or leased by CBNJ, the volunteer, or a third party. All volunteers, contractors, consultants, temporary, and other workers at CBNJ and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with CBNJ policies and standards, and local laws and regulation.

This policy applies to any volunteers and other workers at CBNJ, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by CBNJ.

# **4.** **Policy**

## **4.1** **General Use and Ownership**

## 4.1.1 CBNJ proprietary information stored on electronic and computing devices whether owned or leased by CBNJ, the volunteer or a third party, remains the sole property of CBNJ. You must ensure through legal or technical means that proprietary information is protected in accordance with the *Data Protection Standard.*

## 4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of CBNJ proprietary information.

## 4.1.3 You may access, use or share CBNJ proprietary information only to the extent it is authorized and necessary to fulfill your assigned duties.

## 4.1.4 Volunteers are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, volunteers should be guided by departmental policies on personal use, and if there is any uncertainty, volunteers should consult their leaders.

## 4.1.5 For security and network maintenance purposes, authorized individuals within CBNJ may monitor equipment, systems and network traffic at any time.

## 4.1.6 CBNJ reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

**4.2** **Security and Proprietary Information**

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Minimum Access Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less. You must lock the screen or log off when the device is unattended.

4.2.4 Postings by volunteers from a CBNJ email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of CBNJ, unless posting is in the course of business duties.

4.2.5 Volunteers and personnel must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

**4.3** **Unacceptable Use**

The following activities are, in general, prohibited. Volunteers 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).

Under no circumstances is a Volunteer of CBNJ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing CBNJ-owned resources.

The lists below are by no means exhaustive, but attempt to provide 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, with no exceptions:

1. 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 CBNJ.
2. Unauthorized 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 CBNJ or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting CBNJ business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a CBNJ computing asset 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.
8. Making fraudulent offers of products, items, or services originating from any CBNJ account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the volunteer is not an intended recipient or logging into a server or account that the volunteer is not expressly authorized to access, unless these duties are within the scope of regular duties. 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.
11. Port scanning or security scanning is expressly prohibited unless prior notification to Infosec is made.
12. Executing any form of network monitoring which will intercept data not intended for the volunteers host, unless this activity is a part of the volunteers duty.
13. Circumventing user authentication or security of any host, network or account.
14. Introducing honeypots, honeynets, or similar technology on the CBNJ network.
15. Interfering with or denying service to any user other than the volunteers host (for example, denial of service attack).
16. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, by any means, locally or via the Internet/Intranet/Extranet.
17. Providing information about, or lists of, CBNJ volunteers to parties outside CBNJ

4.3.2 Email and Communication Activities

When using church resources to access and use the Internet, users must realize theyrepresent the company. Whenever volunteers state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the company". Questions may be addressed to the IT Department

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within CBNJ's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by CBNJ or connected via CBNJ's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by volunteers, whether using CBNJ’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of CBNJ’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate CBNJ’s policy, is not detrimental to CBNJ’s best interests, and does not interfere with an employee's regular work duties. Blogging from CBNJ’s systems is also subject to monitoring.

2. CBNJ’s Confidential Information policy also applies to blogging. As such, Volunteers are prohibited from revealing any CBNJ confidential or proprietary information, trade secrets or any other material covered by CBNJ’s Confidential Information policy when engaged in blogging.

3. Volunteers shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of CBNJ and/or any of its employees. Volunteers are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by CBNJ’s *Non-Discrimination and Anti-Harassment* policy.

4. Volunteers may also not attribute personal statements, opinions or beliefs to CNMJ’s when engaged in blogging. If anyone is expressing his or her beliefs and/or opinions in blogs, they may not, expressly or implicitly, represent themselves as a representative of CBNJ. Volunteers assume any and all risk associated with blogging.v

**5.** Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, CBNJ’s trademarks, logos and any other CBNJ intellectual property may also not be used in connection with any blogging activity

**4.4 Password Policy**

1. Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 14 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words. Examples include “*It’s time for vacation*” or “*block-curious-sunny-leaves*”. Passphrases are both easy to remember and type, yet meet the strength requirements. Poor, or weak, passwords have the following characteristics:

· Contain eight characters or less.

· Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.

· Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.

· Are some version of “Welcome123” “Password123” “Changeme123”

1. In addition, every work account should have a different, unique password. To enable users to maintain multiple passwords, we highly encourage the use of ‘password manager’ software that is authorized and provided by the organization. Whenever possible, also enable the use of multi-factor authentication.

**4.5 Data Breach Response Policy**

**Policy Confirmed theft, data breach or exposure of CBNJ’s Protected data or CBNJ’s Sensitive data**

As soon as a theft, data breach or exposure containing CBNJ Protected data or CBNJ Sensitive data is identified, the process of removing all access to that resource will begin.

The Executive Director will chair an incident response team to handle the breach or exposure.

The team will include members from:

• IT Infrastructure

• IT Applications

• Finance (if applicable)

• Legal

• Communications

• Member Services (if Member data is affected)

• Human Resources

• The affected unit or department that uses the involved system or output or whose data may have been breached or exposed

• Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of CBNJ data

The Executive Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

**Work with Forensic Investigators**

As provided by CBNJ cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

**Develop a communication plan.**

Work with CBNJ communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

**1. Ownership and Responsibilities**

Roles & Responsibilities:

• Sponsors - Sponsors are those members of the CBNJ community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any CBNJ Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.

• Information Security Administrator is that member of the CBNJ community, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.

• Users include virtually all members of the CBNJ community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.

• The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

**2. Enforcement**

Any CBNJ personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

**4.6 Internet Usage Policy**

1 Resource Usage  
Access to the Internet will be approved and provided only if reasonable church needs are identified. Internet services will be granted based on a volunteer's current job responsibilities.

4.2 Allowed Usage

Internet usage is granted for the sole purpose of supporting church activities necessary to carry out job functions. All users must follow the corporate principles regarding resource usage and exercise good judgment in using the Internet. Questions can be addressed to the IT Department.

Acceptable use of the Internet for performing job functions might include:

* Communication between employees and non-employees for chruch purposes;
* IT technical support downloading software upgrades and patches;
* Review of possible vendor web sites for product information;
* Reference regulatory or technical information.
* Research

3 Personal Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user’s manager and the IT department, may be considered cause for disciplinary action.  
  
All users of the Internet should be aware that the church network creates an audit log reflecting requests for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk. The church is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property

4 Prohibited Usage

Information stored in the wallet, or any consequential loss of personal property.

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libelous materials.

Other activities that are strictly prohibited include, but are not limited to:

* Accessing church information that is not within the scope of one’s work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.
* Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.
* Deliberate pointing or hyper-linking of church Websites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of the company.
* Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law including without limitations US export control laws and regulations.
* Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.
* Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
* Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libelous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.
* Any form of gambling.

Unless specifically authorized under the provisions of section 3, the following activities are also strictly prohibited:

* Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user’s manager.
* Any ordering (shopping) of items or services on the Internet.
* Playing of any games.
* Forwarding of chain letters.
* Participation in any on-line contest or promotion.
* Acceptance of promotional gifts.

Bandwidth both within the church and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other volunteers.

5 Software License

The company strongly supports strict adherence to software vendors’ license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor’s license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

Using church computer resources to access the Internet for personal purposes, without approval from the user’s manager and the IT department, may be considered cause for disciplinary action.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet "wallets" do so at their own risk.

6 Review of Public Information

All publicly-writable directories on Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with company business. Examples of unauthorized public information include pirated information, passwords, credit card numbers, and pornography.

7 Expectation of Privacy

7.1 Monitoring

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.  
  
Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

7.2 E-mail Confidentiality

Users should be aware that clear text E-mail is not a confidential means of communication. The church cannot guarantee that electronic communications will be private. Volunteers should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

8 Maintaining Corporate Image

8.1 Representation

When using church resources to access and use the Internet, users must realize theyrepresent the church. Whenever employees state an affiliation to the company, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the church". Questions may be addressed to the IT Department.

8.2 Church Materials

Users must not place church material (examples: internal memos, press releases, product or usage information, documentation, etc.) on any mailing list, public news group, or such service. Any posting of materials must be approved by the employee’s manager and the public relations department and will be placed by an authorized individual.

9 Periodic Reviews

9.1 Usage Compliance Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

9.2 Policy Maintenance Reviews

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs.

# **5.** **Policy Compliance**

5.1 Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

# 5.2 Exceptions

Any exception to the policy must be approved by the IT team in advance.

# 5.3 Non-Compliance

A volunteer found to have violated this policy may be subject to disciplinary action.

# **6.** **Related Standards, Policies and Processes**

* Data Classification Policy
* Data Protection Standard
* Social Media Policy
* Minimum Access Policy
* Password Policy
* Router and Switch Security Policy
* Internet Usage Policy

# **7.** **Definitions and Terms**

The following definition and terms can be found in the SANS Glossary located at:

<https://www.sans.org/security-resources/glossary-of-terms/>

<https://fraudfighting.org/wp-content/uploads/2017/12/Email-Bombing-and-Spamming.pdf>

<https://www.directives.doe.gov/terms_definitions/proprietary-information>

· Blogging

· Honeypot

· Honeynet

· Proprietary Information

· Spam

· Viruses

· Worms

· Trojan horses

· E-mail bombs

**8.** **Revision History**

|  |  |  |
| --- | --- | --- |
| **Date of Change** | **Responsible** | **Summary of Change** |
| October 21,2020 | CBNJ Policy Team | Updated and converted to new format |
|  |  |  |

# 