ANGLICAN DIOCESE
OF ISLANDS AND INLETS

p 250.386.7781
w bc.anglican.ca

Information Security Policy

1. INTRODUCTION

In order to provide a variety of services to the many parishes that make up our diocese we have turned to technology for assistance. The synod office has established an information sharing system that utilizes electronic mail, among other applications, as a primary communication medium between the synod office and the various parish administrative offices throughout our region.

Due to the nature of the information that flows between the synod office and individual parishes, it is imperative that well managed information security controls be in place to protect the integrity, privacy and confidentiality of sensitive information.

The diocese, including its offices, agencies, parishes, employees, volunteers and other representatives, will adhere to the diocesan Privacy Policy and the provisions of the Personal Information Protection Act (PIPA) relating to the collection, accuracy, protection, use, retention, archival transfer and disclosure of personal information.

2. DEFINITIONS

"Diocese" means the Anglican Diocese of British Columbia and, where the context requires, includes its member parishes and other organizations.

"Sensitive Information" means information, in electronic or hard-copy form, that has been created, received, collected or stored by or on behalf of the diocese and has been classed confidential, restricted or internal use under section 9.

"User" means any employee, contractor, temporary employee or volunteer of the synod, a parish, or any other diocesan organization, who produces, receives, has access to, disseminates or stores Sensitive Information.

3. INFORMATION SECURITY AND AWARENESS TRAINING

Every user will be required to be aware of the vital need for information security when engaged in any activities related to the business of the diocese.

At the commencement of employment or involvement, users will receive an orientation from their supervisor that will highlight:

1. the need for information security

2. the responsibility of everyone within the diocese to observe best practices related to information security.
3. the requirement to execute a signed acknowledgement as a formal undertaking to practice personal responsibility to safeguard the diocesan business flow of information. This would include any business or personal information access as part of the duties assigned as a basic work ethic.

This information security awareness requirement will be reinforced on a frequent basis from the chief security officer. This reinforcement will consist of various types of collateral (letters, posters, memos, meetings, and promotions) created and supported by the synod office.

This awareness will be instituted at commencement of employment and reviewed on an annual basis. In the case of employees, this review shall coincide with performance reviews. Reviews shall also be required when there is a substantive change in the diocesan information technology environment. Established users are expected to take part in this information security awareness orientation as if they were newly recruited to their position. This awareness reinforcement program will be managed and monitored by the synod office.

Suitable user-friendly reference material will be made available as part of the awareness program content.

4. USE OF ANTI-VIRUS SOFTWARE

In order to protect against the inadvertent introduction of malicious software, every device shall be equipped with a current, industry standard, anti-virus (aka anti malicious software) program that is properly maintained and updated. All desktops and portable computing devices will adhere to this anti virus standard. Maintenance of the virus signature files is under the control and responsibility of those tasked with desktop support. This group will routinely update all Synod connected desktops and portable computing devices as new anti-virus signatures become available. It is the responsibility of each parish or other diocesan organization to ensure that their anti-virus definitions are kept up to date.

5. INVOLVED PERSONS

All matters related to information security will come under the direct control and management of the diocesan executive officer, acting in the role of chief security officer. All personnel issues related to information security will be referred to the executive officer for resolution.

Synod office staff shall create and maintain a list of users, which will become the basis for providing each qualified user with an ability to use and access the information and technology resources of the synod office according to a pre-determined level of access rights. Each parish or other diocesan organization will be responsible for keeping its own list of users up to date, and for providing timely updates to the diocesan communications officer.

It is the responsibility of the chief security officer to ensure that every User receives a copy of this policy and all other related policies as part of their responsible use of information and the Diocesan technology. Synod office will require that each such User individual is made familiar with these policy documents, that they read and acknowledge understanding of the policy directives and attest to this fact by signing the acknowledgement referred to in section 3 above.

6. USER ACCOUNTABILITY AND PASSWORD MANAGEMENT

Password access control for authentication shall be unique to each User and serves, not only as their access credentials, but also as a tracking mechanism for after the fact accountability for actions related to information security and privacy. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized User. Information Technology support staff must never ask Users to reveal their passwords.

To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess. These passwords must not be recorded on any medium that can be compromised

Passwords must be updated at regular intervals, to be determined by the chief security officer. Users shall not re-use passwords on an obsolete list, that is, within the last 10 on a list of used passwords. A password history database will remember expired passwords, and a User cannot create a new password that is one of those on the history file until the last one expires.

Passwords must meet complexity requirements. These requirements are as follows:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
- Must not be a dictionary word, personal history detail, name, or reflection of work activities;
- Be at least six characters in length; and,
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z);
    - English lowercase characters (a through z);
    - Base 10 digits (0 through 9); or,
    - Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

7. USER IDENTITY

Misrepresenting, obscuring, suppressing, or replacing another User's identity on an electronic mail or other communications system is forbidden. The username, electronic mail address, organizational affiliation, and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

With the exception of hotlines that are intended to be anonymous, users must not send anonymous electronic communications. At a minimum, all users must provide their name and phone number in all electronic communications.

Electronic mail signatures indicating job title, company affiliation, address and other particulars are required for all electronic mail messages. Digital certificates (created through the use of industry standard public and private security keys) are also required for electronic mail of a critical business nature to clearly provide proof of sender and recipient of such sensitive information and transactions.

8. AUTHORIZED USAGE

The diocesan electronic communications systems generally must be used for business activities only. Incidental personal use is permissible as long as it does not consume more than a trivial amount of system resources, does not interfere with worker productivity, and does not preempt any business activity.

The Diocesan electronic communication systems must not be used for personal fund-raising campaigns, political advocacy efforts, religious efforts not related to Diocesan activities, personal business activities, or personal amusement and entertainment.

News feeds, electronic mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to both Diocesan business and the duties of the users.

The use of corporate information system resources must never create the appearance or the reality of inappropriate use.

9. INFORMATION CLASSIFICATION

In order to preserve the appropriate confidentiality, integrity and availability of Diocesan information assets, the Synod office must make sure it is protected against unauthorized access, disclosure or modification. This is not just critical for assets covered by the Personal Information Protection Act, and the primary and secondary data used for research purposes, but also for all business conducted across the diocese. Different types of information require different security measures depending upon their sensitivity. The Diocesan information classification standards are designed to provide users with guidance on how to classify information assets properly and then use them accordingly.

Users and other diocesan community members must respect the security classification of any information as defined and must report any inappropriate situation that could compromise information confidentiality, privacy or integrity to the chief security officer or their designate as quickly as possible.

Information owners are responsible for assessing information and classifying its sensitivity. They should then apply the appropriate controls to protect that information. Information ownership can be delegated.

The synod office, through its IT service provider is responsible for providing the mechanisms or instructions for protecting electronic information while it is resident on any diocesan-owned or controlled system.

Relevant synod staff are responsible for providing the instructions for the protection and preservation of records, whether physical or electronic.

The following definitions provide a summary of the information classification levels that have been adopted by the diocese:

1. CONFIDENTIAL

'Confidential' information has significant value for the diocese, and unauthorized disclosure or dissemination could result in severe financial or reputational damage to the diocese, including fines for data breaches or violation of information confidentiality or privacy. Only those who need explicit access must be granted it, and only to the least degree in order to do their work. When held outside the synod office network, on mobile devices such as laptops, tablets or phones, or in transit, 'confidential' information must be protected behind an explicit logon and by strong encryption shall be as determined by the chief security officer.

2. RESTRICTED

'Restricted' information is subject to controls on access, such as only allowing valid logons from a small group of staff. 'Restricted' information must be held in such a manner that prevents unauthorized access (i.e. on a system

that requires a valid and appropriate user to log in before access is granted). Disclosure or dissemination of this information must be tightly controlled, and a data breach of this type of information may well incur negative publicity and depending on the severity of the data breach could cause severe financial or reputational damage to the diocese.

3. INTERNAL USE

'Internal use' information can be disclosed or disseminated by its owner to appropriate members of the diocese, partners and other individuals, as determined by information owners without any restrictions on content or time of publication.

4. PUBLIC

'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

Designating information as 'confidential' involves significant costs in terms of implementation, hardware and ongoing resources, and makes data less mobile. For this reason, information owners making classification decisions must balance the risk of damage that could result from unauthorized access to, or disclosure of the information against the cost of additional hardware, software or services required to protect it.

This classification system is in effect regardless of the medium that contains the information. Therefore, any paper or facsimile or other means of communication must adhere to the same information classification as computer readable media.

10. LABELING ELECTRONIC MAIL MESSAGES

All electronic mail messages containing sensitive information must include the appropriate classification in the email message header. This label will remind recipients that the information must not be disseminated further or be used for unintended purposes without the proper authorization.

11. ELECTRONIC MAIL SECURITY, PRIVACY AND COMPLIANCE

The diocese will adopt those best practices for the use of e-mail that are consistent with its administration and business goals and which offer the best e-mail security, privacy and compliance required by PIPA mandates and the expectations of diocesan correspondents.

Users and the larger community e-mail users are required to be diligent in the use of diocesan email services to adhere to the fundamental requirement to protect all sensitive information.

12. USE ONLY THE SYNOD ELECTRONIC MAIL SYSTEMS

Unless permission from the chief security officer, or their designate, has been obtained, users must not use their personal electronic mail accounts with an Internet service provider (ISP), electronic mail features found in web browsers, or any other third party for any diocesan business messages. Each authorized email user will be provided with an email identification and account on the diocesan email service to facilitate diocesan email usage.

13. SHARED EMAIL ADDRESSING FOR PARISH ELECTRONIC MAIL

The communications office, in cooperation with its website development service provider, will institute standard shared email addresses for all parishes. The procedure will create email IDs for the following parish positions:

treasurer@domain (the domain name will be @YOUR PARISH CHOSEN DOMAIN NAME)
warden1@domain
admin@domain
incumbent@domain
safechurch@domain
pwrdf@domain

Additional emails may be assigned by the parish office for other ministries as required. Such changes are to be communicated to the synod office as they are made.

Each of these usernames e.g. "treasurer" will be assigned to a named user account e.g. "John Smith" through Microsoft 365 at the commencement of their term in office. Upon completion of the term, the email from the account will be archived and the username (e.g. "treasurer") will be reassigned to the person assuming the position using a new named user account. Named accounts e.g. jsmith@domain will be used to personally identify the user and these accounts will be redirected to the relevant general inbox. Display names include first initial and last name of the individual while the email address retains the standardized term for the position.

These standardized emails are to be used exclusively by synod office and other synod personnel to correspond with parish representatives fulfilling the function of these roles.

Personal email addresses are not to be used or published on the Internet. Personal email addresses are to be published in print only with the consent of the addressee.

14. ADDENDUM ON OUTBOUND ELECTRONIC MAIL

A footer prepared by the legal advisor to the synod office must be automatically appended to all outbound electronic mail originating from synod office computers or authorized users of the synod office email system. This footer must refer to the possibility that the message may contain confidential information, that it is for the use of the named recipients only, that the message has been logged for archival purposes, that the message may be reviewed by parties at the synod office other than those named in the message header, and that the message may not necessarily constitute an official representation of the synod office or the diocese of British Columbia.

In addition, a standard clause will indicate the private nature of the communication and warn unauthorized recipients of their responsibility to destroy such erroneous communication and notify the synod office that this has occurred.

15. USE OF ENCRYPTION PROGRAMS

The use of an acceptable encryption system (to be determined by the chief security officer must be used for any Sensitive Information that is sent in the clear across un-trusted network links.

These encryption systems must protect the Sensitive Information from end to end. They must not involve decryption of the message content before the message reaches its intended destination.

Mobile computers, notebook computers, portable computers, personal digital assistants, and similar computers that store sensitive information emanating from the synod office or from Users must consistently employ file

encryption to protect this sensitive information when it is stored inside these same computers, and when it is stored on accompanying data storage media.

Users of these types of computers who are recipients of sensitive information sent by electronic mail must delete this information from their systems if they do not have encryption software that can properly protect it.

Users must not use encryption for any production electronic communications system unless a backup key or a key escrow system has been established with the cooperation of the chief security officer. Key escrow is intended to allow reconstitution of encrypted messages in the event of the demise or incapacity of the original sender.

16. RESPECTING INTELLECTUAL PROPERTY RIGHTS

Although the Internet is an informal communications environment, the laws for copyrights, patents, and trademarks apply. Users may circulate, repost or reproduce material only after obtaining permission from the source. Users, if they quote material from other sources will do so only if these other sources are properly identified with the appropriate attribution. users must not reveal internal diocesan information on the Internet unless the information has been officially approved for public release. All information acquired from the Internet must be considered suspect until confirmed by another source. Users are cautioned that many information resources found on the Internet are being maintained by volunteers without stringent editing or fact checking. Due diligence is required before complete trust can be determined.

17. RESPECTING PRIVACY RIGHTS

Except as authorized by law and otherwise specifically approved by the chief security officer or their designate, Users must not intercept or disclose, or assist in intercepting or disclosing, electronic communications.

The diocese is committed to respecting the rights of users, including their reasonable expectation of privacy. The diocese also is responsible for operating, maintaining, and protecting its electronic communications networks and will seek support services from reliable third parties.

To accomplish these objectives, it may occasionally be necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications. The diocese may employ content monitoring systems, message logging systems, and other electronic system management tools. By making use of the diocesan systems, users consent to permit all information they store on the diocesan systems to be monitored as may be required and divulged to law enforcement at the discretion of the bishop or designated executive management. The acknowledgment referred to in section 3 above will include the user's express consent to these practices.

18. NO GUARANTEED MESSAGE PRIVACY

The diocese cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others.

Electronic communications may be accessed by people other than the intended recipients in accordance with this policy. Because messages can be stored in backups, electronic communications actually may be retrievable when a traditional paper letter would have been discarded or destroyed. Users must be careful about the topics covered in diocesan electronic communications and must not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.

19. CONTENTS OF MESSAGES

Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing clergy, employees, parishioners or others. Such remarks may create legal problems such as slander, libel or defamation of character.

Users concentrate on business matters in diocesan electronic communications. As a matter of standard business practice, all electronic communications must be consistent with conventional standards of ethical and polite conduct.

20. HANDLING ATTACHMENTS

When sending an attachment to a third party, Users must use pdf, jpg, rich text format or simple text files whenever possible. Users must encourage third parties to send them files in these same formats whenever reasonable and practical. All other attachment files must be automatically scanned with an authorized virus detection software package before opening or execution.

In some cases, attachments must be decrypted or decompressed before a virus scan takes place. Users must be suspicious about unexpected electronic mail attachments received from third parties, even if the third party is known and trusted. No email attachment is to be opened without prior independent verification of its nature and purpose.

21. ARCHIVAL STORAGE

Many documents transmitted and received by the synod office require long term secure storage. An archive has been established for the care and keeping of these documents. It is also necessary to manage the receipt and disposition of some documents that have highly sensitive or important information contained therein. For these reasons the synod office will maintain a logging and tracking procedure to be able to account for every inbound and outbound document of importance.

22. PURGING ELECTRONIC MESSAGES

Messages no longer needed for business purposes must be periodically purged (by users) from their personal electronic message storage areas. The recommended retention period for email messages is six months. After six months systems administration staff will be requested to delete stale-dated messages unless there is an archival requirement.

23. RELATIONSHIP TO OTHER DIOCESAN POLICIES

From time to time additional synod office policies will be issued that may refer to this top-level information security policy. In the case of conflict between this policy and others, this policy shall govern.

24. THIS POLICY ANNUAL MAINTENANCE AND UPDATES

In keeping with the administration management cycle of activity within the synod office this policy will be reviewed at minimum on an annual basis. Changes, additions and updates will be promulgated in a timely manner with a view to synchronizing these activities with the Diocesan Council meetings and Synod.

Users are encouraged to be proactive in forwarding recommended changes, additions and updates to this policy document. All submissions will be carefully reviewed and acknowledged back to the submitter with a disposition as it is deemed appropriate