Security Policy Manual

June 2019

Revision History

Version	Date	Author	Summary of Changes
1.0	06/01/2019	Armand Brunelle	Original Document

Approvals

Table of Contents

1.0 Introduction

Control Number:

Control Objective:

Item Name:

Task:

Gabriel's network within their office is NOT an important resource for achieving our business objectives. All critical resources, such as databases, reseller and vendor information, client data, and user information are areas that must be protected from intrusion and inappropriate use or disclosure. Gabriel uses the Azure protection resources to prevent intrusion and other malicious activities.

The purpose of this policy is to ensure that all individuals utilizing Gabriel's resources understand their responsibility in reducing the risk of compromise and take appropriate security measures to protect our company's systems and data. Everyone at Gabriel has a responsibility to assist with the implementation and enforcement of this policy.

Gabriel will use the appropriate personnel, vendor or affiliate policies to adjudicate violations such as failure to comply with this policy, not taking corrective action when notified, system or network misuse or improper disclosure of protected information.

2.0 Acceptable Use Policy

Control Number:

Control Objective:

Item Name:

Task:

2.1 Overview

Gabriel's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Gabriel's established culture of openness, trust and integrity. Gabriel is committed to protecting our employees, partners and the company 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 Gabriel or are contracted services to Microsoft Azure and/or Microsoft Office 365. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Gabriel employee and affiliate 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. Security procedures are sought from many external sources on an ongoing basis to stay current with new technologies and systems.

2.2 Purpose

This policy outlines the acceptable use of computer equipment at Gabriel for the purpose of protecting Gabriel, Gabriel's employees, clients, and partners. Inappropriate use exposes Gabriel to risks including virus attacks, compromise of network systems and services, and legal issues.

2.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Gabriel, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Gabriel.

2.4 Policy

2.4.1 General Use and Ownership

1. All data that users create on the corporate systems remains the property of Gabriel. Management does not guarantee the confidentiality of personal information stored on any network device belonging to Gabriel.
2. Employees should exercise good judgment regarding the personal use of company assets. In the absence of such policies, employees should be guided by departmental policies on personal use. For questions regarding acceptable usage, employees should consult their supervisor or manager.
3. For security and network maintenance purposes, authorized individuals within Gabriel may monitor equipment, systems and network traffic at any time.
4. Gabriel reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

2.4.2 Security and Proprietary Information

1. The information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in the Information Sensitivity policy. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. User level passwords must be changed at least every 42 days for domain accounts and 90 days for Connections accounts.
3. All users are required to lock the screen (control-alt-delete for Windows users) of their PC, laptop, or workstation when it will be unattended.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Postings by employees from a Gabriel email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Gabriel, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the Gabriel Internet/Intranet/Extranet, whether owned by the employee or Gabriel, shall be continually executing approved virus-scanning software (Symantec Corporate Antivirus Protection) with current virus definitions.
7. Employees should avoid or must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, Trojans, or other forms of malware.

2.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

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

The list items below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

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 Gabriel.

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 Gabriel or the end user does not have an active license is strictly prohibited.
3. 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.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, etc.).
5. Revealing account passwords to others or allowing others usage of an account not their own. This includes family and other household members when work is being done at home.
6. Using a Gabriel 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.
7. Making fraudulent offers of products, items, or services originating from any Gabriel account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Gabriel is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Gabriel employees to parties outside Gabriel unless it is a part of normal job duties.

2.5 Email and Communications Activities

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 Gabriel's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Gabriel or connected via Gabriel's network.
7. Posting the same or similar non-business-related messages to large numbers of email recipients (spam).

2.6 Enforcement

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

2.7 Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings.

3.0 Access Control Policy

Control Number:

Control Objective:

Item Name:

Task:

Gabriel has established the following policy to define how access control to information systems and services cover all stages in the life cycle of user access: from registration of new users to de-registration of users who no longer need access. Where possible, user policies are enforced by the operating system or other software.

- Gabriel data must have sufficient granularity to allow appropriate authorized access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorized purposes. Gabriel recognizes this balance.
- Where possible and financially feasible, more than one person must have full rights to any Gabriel owned server storing or transmitting highly sensitive data. Gabriel has a standard policy that applies to user access rights.
- Access to Gabriel's Azure environment, servers and systems is achieved by individual and unique logins, and requires authentication. Authentication may include the use of passwords, smart cards, biometrics, and/or other recognized forms of authentication. Gabriel uses Microsoft Azure Active Directory and authorization services.
- As stated in Gabriel's policy on appropriate and acceptable use, users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. All users must secure their username or account, password, and system access from unauthorized use.
- All users of Gabriel systems must have a strong password - the definition of which is established in Gabriel's password policy. Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently, consistent with guidelines established in the password policy.
- Default passwords on all Gabriel systems are changed after installation. All administrator or root accounts are given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords are not coded into programs or queries unless they are encrypted or otherwise secure. This information is stored in the Microsoft Azure Vault.
- Terminated employee access is reviewed and adjusted as found necessary. Terminated employees have their accounts disabled upon transfer or termination. Since there could be delays in reporting changes in user responsibilities, periodic user access reviews are conducted by the Network Administrator.
- Transferred employee access is reviewed and adjusted as found necessary.
- Physical access to Gabriel offices is controlled using individual proximity key cards and fobs. There is no system information stored on the office networks. The office networks are just used to facilitate printing and internet access.
- Monitoring has been implemented on all Gabriel systems including recording logon attempts and failures, successful logons and date and time of logon and logoff. Physical Security Policy

Control Number:

Control Objective:

Item Name:

Task:

3.1 Purpose

The purpose of the Gabriel Physical Security Policy is to establish the rules of granting, controlling, monitoring, and removing physical access to Gabriel's facilities, property and equipment.

3.2 Scope

The Physical Security Policy applies to all individuals that have been granted access to Gabriel's facilities, property and equipment. NOTE: Gabriel office networks do not have system or customer information. Platform is Microsoft Azure based.

3.3 Policy

Gabriel resources must be physically protected in proportion to the criticality, sensitivity, or business importance of their function(s) keeping in mind that all sensitive data and data processing is done in the Microsoft Azure Cloud.

- All physical security systems must comply with all applicable regulations, including, but not limited to, building codes and fire prevention codes.
- Restricted areas and facilities must be clearly marked. Signage for restricted areas and facilities should contain enough information to be practical, but present minimal discernible evidence as to the nature of the importance of the location.
- Each individual granted physical access to restricted Information Resources or facilities must receive training on emergency procedures for the facility.

3.3.1 Surveillance

- Physical access to all restricted Information Resources and facilities must be documented.
- All facilities that allow visitors must track visitor access with a sign in/sign out log.
- Card access records and visitor logs for Information Resources facilities must be kept for routine review based upon the criticality of the Information Resources being protected.
- The Security Administrator must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.
- Gabriel employs video surveillance technology to deter theft, violence and other criminal activity.
    - In the event of a reported or observed incident, the recorded footage may be used to assist in the investigation of the incident and may be turned over to law enforcement personnel, if appropriate.

- At no time will persons other than those designated have access to the footage made in the course of surveillance. Personal information contained on the footage shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
- Footage from the surveillance cameras will be kept until the database reaches its storage limits; the oldest data will be purged first unless required for the purposes outlined in this policy. If footage has been used to investigate an incident, that footage will be retained for one year after a final decision is reached concerning the incident.
- Old footage that isn't reused or recycled for surveillance will be shredded, burned, or otherwise made permanently unreadable.

3.3.2 Security Access System

- Personnel, including full- and part-time staff, contractors, and vendor service staff, should be granted access only to facilities and systems necessary to fulfill their job responsibilities.
- Requests for access must come from and include sign-off from an applicable data/system owner.
- The process for granting physical access to Information Resources facilities must include the approval of the Security Administrator.
- Each individual granted physical access to an Information Resources facility must sign appropriate access, information protection, and nondisclosure agreements.
- The Help Desk must remove card and/or key access rights of individuals that leave or change roles within Gabriel.
- The Help Desk reviews card and/or key access rights for the facility on a quarterly basis as a part of the Security Access Audit and remove access for individuals that no longer require access.
- Visitors who have not been granted special access privileges must at all times be escorted and monitored in access-controlled areas at Gabriel facilities.

3.3.3 Protection of physical access cards and keys

- Personnel must not share or transfer access cards and/or to other individuals within or external to Gabriel including "piggybacking" i.e. allowing fellow employees or other individuals to follow into an access controlled area without appropriate permissions.
- Access cards and/or keys that are no longer needed must be returned to the Help Desk. Cards must not be transferred or reallocated to another individual, bypassing the return process.
- Lost or stolen access cards and/or keys must be reported to the Help Desk.
- A service charge may be assessed for access cards and/or keys that are lost, stolen, or not returned.

3.4 Enforcement

Gross negligence or willful disregard of this standard may result in disciplinary action which may include loss of Gabriel access privileges, termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals may be subject to civil and criminal prosecution.

4.0 Anti-Virus Software Policy

Control Number:

Control Objective:

Item Name:

Task:

- All workstations and servers owned and operated by Gabriel are required to run the Windows Defender Antivirus software.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying the computer's Recycle Bin.
- Delete spam, chain, and other junk email without forwarding, as per Gabriel's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan removable disks from an unknown source for viruses before using them.
- If testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the test. After the test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
- New viruses are discovered almost every day. Virus definitions are automatically updated daily by Symantec Corporate Antivirus.

5.0 Automatically Forwarded Email Policy

Control Number:

Control Objective:

Item Name:

Task:

5.1 Purpose

To prevent the unauthorized or inadvertent disclosure of sensitive company information.

5.2 Scope

This policy covers automatic email forwarding, and thereby the potentially inadvertent transmission of sensitive information by all employees, vendors, and agents operating on behalf of Gabriel.

5.3 Policy

Employees must exercise utmost caution when sending any email from inside Gabriel to an outside network. Unless approved by an employee's manager, Gabriel's email will not be automatically forwarded to an external destination. Sensitive information, as defined in the Information Sensitivity Policy, will not be forwarded via any means, unless that email is critical to business.

5.4 Enforcement

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

5.5 Definitions

Terms	Definitions
Email	The electronic transmission of information through a mail protocol such as SMTP. Programs such as Microsoft Outlook use SMTP.
Forwarded email	Email resent from internal networking to an outside point.
Sensitive information	Information is considered sensitive if it can be damaging to Gabriel or its customers' dollar value, reputation, or market standing.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people who do not have a need to know that information.

6.0 Backup / Restore Policy

Control Number:

Control Objective:

Item Name:

Task:

6.1 Overview

This policy defines the backup policy for computers within Gabriel which have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers backed up include file, mail, database, application, and web.

6.2 Purpose

This policy is designed to protect data within Gabriel to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

6.3 Scope

This policy applies to all equipment and data owned and operated by Gabriel, Inc.

6.4 Definitions

Term	Definition
Backup	The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
Archive	The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
Restore	The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

6.5 Timing

Full data replication of all Azure Gabriel SQL Server Datbases are done in real time.

Gabriel does not utilize tape backup. All backup is done disk to disk over our 45 Mbps point to point DS3 to an offsite storage location (See 6.11). All back up sets are encrypted using an AES 128bit encryption key.

6.6 Responsibility

Backup success and failure reports are emailed to Production-Alarms and the System Administrator. All failures are monitored by the System Administrator and the IT management team. Errors are corrected and a manual backup is run upon backup failure.

6.7 Testing

The ability to restore data from backups shall be tested at least once per quarter using actual test restores.

6.8 Data Backed Up

Data to be backed up include the following information:

1. Transaction data within the SQL Server databases on the Azure platform

Other unstructured data such as word documents, excel documents (etc) are stored in Microsoft O365 SharePoint and One Drive locations which are backed up automatically by Microsoft.

6.9 Restoration

Users that need files restored must submit a change request to the IT Infrastructure department. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

6.10 Documentation Review

Gabriel's Network Administrator ensures that backup documentation is kept current by performing a quarterly review of documentation or designating a staff member to perform a review.

7.0 Operational and Software Development Change Management Policy

Control Number:
Control Objective:
Item Name:
Task:

****** this policy is contained in a separate Change Management Policy Document ******

8.0 Password Policy

Control Number:

Control Objective:

Item Name:

Task:

8.1 Overview

All Gabriel employees (including contractors and vendors with access to Gabriel systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

8.2 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

8.3 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Gabriel facility, has access to the Gabriel network, or stores any non-public Gabriel information.

8.4 Policy

8.4.1 General

- All system-level passwords (e.g., root, administrator, application administration accounts, etc.) must be changed on at least a quarterly basis.
- User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

8.4.1.1 Password Protection Standards

Do not use the same password for Gabriel accounts as for other non-Gabriel access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Gabriel access needs.

Do not share Gabriel passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Gabriel information.

Here is a list of "don’ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss

- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call the Help Desk.

Do not use the "Remember Password" feature of Windows or applications (e.g., Internet Explorer, Outlook, Netscape, etc.).

Again, do not write passwords down and store them anywhere in the office. Do not store passwords in a file on ANY computer system (including Blackberrys or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident and change all passwords.

Administrative password cracking or guessing may be performed on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it.

8.4.1.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

8.4.1.3 Use of Passwords and Shared Keys for Remote Access Users

Access to the Gabriel network via remote access (VPN) is to be controlled using either password authentication or a shared key system managed by a VPN client.

8.4.1.4 Two Factor Authentication is REQUIRED for all Gabriel Office 365 and Gabriel Active Directory accounts

With each login, users will be prompted to type in a code that has been texted to their mobile phone.

8.4.2 Active Directory

- Change passwords every 42 days (except system-level passwords which must be changed at least quarterly).
- Users cannot reuse any of their last 24 passwords.
- Password must be a minimum of 7 characters; it must contain one capital letter or special character and at least one number.

8.4.3 Connections

- New users receive a temporary password that needs to be changed every 90 days
- Users cannot reuse their previous password when prompted to change it
- Passwords must be a minimum of 6 characters; passwords require at least one capital letter and one number
- Passwords are encrypted using a 128 bit RC4 stream cipher during transmission to the server and are stored in the database using a secure 160-bit SHA hash value. This secure hash means that although passwords may be reset by an administrator they can never be retrieved from the database.

8.4.4 MultiView Financials

- New users receive a temporary password that needs to be changed when they first log in
- Users must change their passwords every 60 days and cannot reuse the last 5 iterations of their passwords
- Passwords must be a minimum of 7 characters; passwords are case sensitive, require at least an uppercase letter and a number, and do not allow repeated characters,

8.5 Enforcement

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

8.6 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., SQL Server database administrator).

9.0 Database Password Policy

Control Number:

Control Objective:

Item Name:

Task:

9.1 Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of Gabriel's networks.

Computer programs running on Gabriel's networks often require the use of one of the internal database servers. In order to access one of these databases, a program must authenticate to the database by presenting acceptable credentials. The database privileges that the credentials are meant to restrict can be compromised when the credentials are improperly stored.

9.2 Scope

This policy applies to all software that will access a Gabriel, multi-user production SQL Server database.

9.3 Policy

9.3.1 General

In order to maintain the security of Gabriel's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server. Specific Requirements

9.3.1.1 Storage of Database User Names and Passwords

- All database passwords are stored in the Microsoft Azure Vault
- Database credentials may not reside in the documents tree of a web server.
- Passwords or pass phrases used to access a database must adhere to the Password Policy.

9.3.1.2 Retrieval of Database User Names and Passwords

- System users are not available for interaction login
- The System Users will access the Vault to acquire the necessary paswords to perform its task

9.3.1.3 Access to Database User Names and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.
- Database passwords used by programs are system-level passwords as defined by the Password Policy.

- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

9.4 Enforcement

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

9.5 Definitions

Term	Definition
Computer language	A language used to generate programs.
Credentials	Something a user knows (e.g., a password or pass phrase), and/or something that identifies a user as being present for authentication (e.g., a user name, a fingerprint, voiceprint, retina print).
Entitlement	The level of privilege that has been authenticated and authorized. The privileges level at which to access resources.
Executing body	The series of computer instructions that the computer executes to run a program.
Hash	An algorithmically generated number that identifies a datum or its location.
LDAP	Lightweight Directory Access Protocol, a set of protocols for accessing information directories.
Module	A collection of computer language instructions grouped together either logically or physically. A module may also be called a package or a class, depending upon which computer language is used.
Name space	A logical area of code in which the declared symbolic names are known and outside of which these names are not visible.
Production	Software that is being used for a purpose other than when software is being implemented or tested.

10.0 Email Retention Policy

Control Number:

Control Objective:

Item Name:

Task:

10.1 Purpose

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction. Questions about the retention of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to the Internal Help Desk.

10.2 Scope

IT provides the infrastructure for departments to retain emails. Each department is responsible for retaining its own emails according to its own policies.

10.3 Policy

10.3.1 Categories of Correspondence

Categories of correspondence that users should use when considering whether to retain an email include:

- Administrative – clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations.
- Fiscal – information related to revenue and expense for the company.
- Ephemeral – personal email, requests for recommendations or review, email related to product development, updates and status reports.
- General – information that relates to customer interaction and the operational decisions of the business.
- Protected Health Information – any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

10.3.2 Instant Messenger Correspondence

Gabriel Instant Messenger correspondence may be saved with logging function of Instant Messenger. Important conversations should be copied and saved in a file on a backed up drive or in an email.

10.3.3 Server Email Retention and Backup

Gabriel used Office 365 standard email retention policy.

10.4 Enforcement

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

10.5 Definitions

Term	Definition
Approved Electronic Mail	Includes all mail systems supported by Systems & Security. For business needs that require the use of other systems, contact the appropriate support organization.
Approved Instant Messenger	Microsoft IM and Spark are the only IM clients approved for use on Gabriel's computers.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac's and PCs, this includes using passwords on screensavers.
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Gabriel.

11.0 Encryption Policy

Control Number:

Control Objective:

Item Name:

Task:

11.1 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those times when users need to send or receive sensitive information. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

11.2 Scope

This policy applies to all Gabriel employees and affiliates.

11.3 Policy

Proven, standard algorithms such as 3DES, RSA, and RC5 should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, PGP Corporation's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 128 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Gabriel's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question. Be aware that the U.S. Government restricts the export of encryption technologies. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Currently Gabriel uses Voltage secure email sending via micro focus cloud system

11.4 Enforcement

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

11.5 Definitions

Term	Definition

12.0 Extranet Policy

Control Number:

Control Objective:

Item Name:

Task:

12.1 Purpose

This document describes the policy under which third party organizations connect to Gabriel networks for the purpose of transacting business related to Gabriel.

12.2 Scope

Currently there are NO external partner connections allowed to the Gabriel network. All external partners receive data via the Gabriel platform. If we were to grant access in the future we would follow the policy below.

12.3 Policy

12.3.1 Pre-Requisites

12.3.1.1 Security Review

All new extranet connectivity will go through a security review by IT management. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least required access is followed.

12.3.1.2 Business Case

All production extranet connections must be accompanied by a valid business justification, in writing, that is approved by IT management. Typically this function is handled as part of the Third Party Agreement.

12.3.1.3 Point of Contact

The Sponsoring Organization must designate a person to be the Point of Contact (POC) for the Extranet connection. The POC acts on behalf of the Sponsoring Organization, and is responsible for those portions of this policy and the Third Party Agreement that pertain to it. In the event that the POC changes, the relevant extranet organization must be informed promptly.

12.3.2 Establishing Connectivity

Sponsoring Organizations within Gabriel that wish to establish connectivity to a third party are to file a new site request with the proper extranet group. The extranet group will engage IT management to address security issues inherent in the project.

All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Gabriel rely upon the third party to protect Gabriel's network or resources.

12.3.3 Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Changes are to be implemented via corporate

change management process. The Sponsoring Organization is responsible for notifying IT management when there is a material change in their originally provided information so that security and connectivity evolve accordingly.

12.3.4 Terminating Access

When access is no longer required, the Sponsoring Organization within Gabriel must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must conduct an audit of their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are found to be depreciated, and/or are no longer being used to conduct Gabriel business, will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct Gabriel business necessitate a modification of existing permissions, or termination of connectivity, IT management will notify the POC or the Sponsoring Organization of the change prior to taking any action.

12.4 Enforcement

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

12.5 Definitions

Term	Definition
Circuit	For the purposes of this policy, circuit refers to the method of network access, whether it's through traditional T1, cable, or via VPN/Encryption technologies.
Sponsoring Organization	The Gabriel organization who requested that the third party have access into Gabriel.
Third Party	A business that is not a formal or subsidiary part of Gabriel.

13.0 Incident Handling Policy

Control Number:

Control Objective:

Item Name:

Task:

****** this policy is contained in a separate Incident Response Policy Document ******

14.0 Incident Response Guidelines

Control Number:

Control Objective:

Item Name:

Task:

****** this policy is contained in a separate Incident Response Policy Document ******

15.0 Information Sensitivity Policy

Control Number:

Control Objective:

Item Name:

Task:

15.1 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Gabriel without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that employees can take to protect Gabriel Confidential information (e.g., Gabriel Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to a manager. Questions about these guidelines should be addressed to Human Resources.

15.2 Scope

All Gabriel information is categorized into two main classifications:

- Gabriel Public
- Gabriel Confidential
    - Client Confidential (subset of Gabriel Confidential)

Gabriel Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Gabriel, Inc.

Gabriel Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in Gabriel Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Gabriel Confidential information is "Client Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Gabriel by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this

category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Gabriel's network to support our operations.

Gabriel personnel are required to secure Gabriel Confidential (as well as subset Client Confidential) information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager immediately.

15.3 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Gabriel Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Gabriel Confidential information in question.

Marking is at the discretion of the owner or custodian of the information. Even if no marking is present, Gabriel information is presumed to be "Gabriel Confidential" unless expressly determined to be Gabriel Public information by a Gabriel employee with authority to do so.

15.3.1 Minimal Sensitivity – "Gabriel Public": General corporate information; some personnel and technical information

Access: Gabriel employees, contractors, people with a business need to know.

Distribution within Gabriel: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Gabriel internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Gabriel premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

15.3.2 More Sensitive – "Gabriel Confidential": Business, financial, technical, and most personnel information

Access: Gabriel employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within Gabriel: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of Gabriel internal mail: Sent via U.S. mail or approved private carriers.

15.3.3 Electronic distribution: No restrictions to approved recipients within Gabriel, but should be encrypted or sent via a private link to approved recipients outside of Gabriel premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In disposal bins on Gabriel premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

15.3.4 Most Sensitive – Elements of "Gabriel Confidential" and all "Client Confidential": Trade secrets & marketing, operational, personnel, financial, source code, & technical Information integral to the success of our company and all Client Confidential Data

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Gabriel Confidential information is very sensitive, consider labeling the information with "Gabriel Internal: Registered and Restricted", "Gabriel Eyes Only", "Gabriel Confidential" or similar labels as deemed by the affected individual business unit or department. Once again, this type of Gabriel Confidential information need not be marked, but users should be aware that this information is extremely sensitive and must be protected as such.

Access: Only those individuals (Gabriel employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within Gabriel: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Gabriel internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within Gabriel, but all "Confidential" information must be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In disposal bins on Gabriel premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

15.4 Enforcement

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

15.5 Definitions

Terms	Definitions
Appropriate measures	To minimize risk to Gabriel from an outside business connection, Gabriel computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Gabriel corporate information, the amount of information at risk is minimized.
Configuration of Gabriel-to-other business connections	Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.
Approved Electronic File Transmission Methods	Includes supported FTP clients and Web browsers.
Envelopes Stamped Confidential	Special envelopes are not required. Put the document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.
Approved Electronic Mail	Includes all mail systems supported by the Network Administrator. These include, but are not necessarily limited to Microsoft Exchange and Outlook. For business needs that require the use of other mailers contact the appropriate support organization.
Approved Encrypted email and files	Techniques include the use of PGP or GPG. DES encryption is available via many different public domain packages on all platforms. Please contact the Help Desk regarding approved encryption methods.
Company Information System Resources	Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.
Expunge	To reliably erase or expunge data on a PC, a separate program must overwrite data. Otherwise, the PC's normal erasure routine keeps the data intact until overwritten.
Individual Access Controls	Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On PCs, this includes using passwords on screensavers.

Terms	Definitions
Insecure Internet Links	Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Gabriel.
Encryption	Secure Gabriel Sensitive information in accordance with the Acceptable Encryption Policy. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult the Help Desk for further guidance.
Physical Security	Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state. Methods of accomplishing this include having a domain username and password to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or keep it in person. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet. No information, equipment, or software belonging to Gabriel shall be removed from the premises without express authorization from executive management.
Private Link	A Private Link is an electronic communications path that Gabriel has control over its entire distance. For example, all Gabriel networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer has established a private link. Connections to employee's homes are private links.

16.0 Media Disposition Policy

Control Number:

Control Objective:

Item Name:

Task:

16.1 Purpose

This document provides specific guidance on methods, processes and procedures to ensure no data remains on removable storage devices that are to be permanently removed from Gabriel.

16.2 Methods for media sanitization and clearing

Overwriting is the process of replacing information (data) with meaningless data in such a way that meaningful information cannot be recovered from a device. The Gabriel technician performing the overwriting will have suitable technical expertise and will be responsible for certifying that the process has been successfully completed.

Destruction of a device is the process of physically damaging a medium so that it is not usable in a computer and so that no known exploitation method can retrieve data from it.

Clearing data (deleting files) simply removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing Gabriel controlled storage media.

16.3 Disposition

Storage devices may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

17.0 Removable Media Policy

Control Number:

Control Objective:

Item Name:

Task:

17.1 Overview

Removable media can be classified as any portable device that can be used to store and/or move data. Media devices can come in various shapes and forms, including USB memory sticks, floppy disks, read/write compact disks and DVDs, PDA storage cards, magnetic tapes and cassettes – essentially anything that can be copied, saved, and/or written to which can then be taken away and restored on another computer.

By design, removable media create their own security vulnerabilities – they provide the means to conveniently transport up to several gigabytes of data from one computer or network to another. The most salient vulnerabilities being:

1) Most forms of removable media require no form of authentication, password protection, or configuration to install or use and they can make use of “plug and play” technologies and generally do not require any administrator privileges to install.
2) Unauthorized disclosure of sensitive data could occur if an item of removable media fell into the wrong hands.
3) In addition to their authorized data, users may also inadvertently transport (and therefore introduce) malicious software on to Gabriel’s systems.
4) The nature and tangible size of removable media is such that they are also prone to accidental loss and/or theft.

17.2 Restrictions for the Management of Removable Media

1) Only Gabriel owned and managed removable media should be used with Gabriel systems.
2) It is not permissible to use Gabriel owned media on personal computers or other devices that do not have an official connection to Gabriel networks.
3) High sensitivity data must be protected to 128bit encryption levels when stored on removable media. If it is not possible to achieve this level of encryption, then its storage is prohibited.
4) Removable media should only be used to transport or store data when other more secure means (internal email or network shares) are not available.
5) If any item of removable media is no longer required by Gabriel, it must be destroyed by approved secure means. This is only to be carried out by the Help Desk.
6) When transferring data from outside of Gabriel, extreme caution must be taken, as the potential impact of a malicious software attack on Gabriel’s systems could be severe.
7) Any loss or theft of any item of removable media must be reported immediately to the Help Desk so that the level of compromise can be assessed, and necessary efforts can be made for recovery.

17.3 Enforcement

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

18.0 Risk Assessment Policy

Control Number:

Control Objective:

Item Name:

Task:

****** this policy is contained in a separate Risk Assessment Policy Document ******

19.0 Source Code Control Policy

Control Number:

Control Objective:

Item Name:

Task:

****** this policy is contained in a separate Change Management Policy Document ******

20.0 Third Party Access

20.1 Purpose

All consultants, contractors, vendors, and outside parties such as law firms, hereinafter referred to as “Third Party” or “Third Parties” who access data hosted by Gabriel must comply with this policy. All Gabriel Third Parties must secure against unauthorized network or physical access, damage or interference to Gabriel’s business operations assets, including but not limited to confidential client information and IT resources. Gabriel Third Parties are subject to applicable requirements of this policy when they perform work for Gabriel or its clients. Gabriel Third Parties who violate this policy will be subject to termination of access and investigation and may result in breach of contract or other penalties.

20.2 Third Party Access General requirements

1. All Third Parties must sign a non-disclosure / confidentiality agreement.

2. Third Parties may only access network and system resources by approved methods.

3. Third Parties must ensure basic security methodologies are in place within their infrastructure (firewall, user access control, etc.).

4. Individuals working for Third Parties are not allowed to share accounts or passwords.

5. Third Parties must ensure that any device connecting to Gabriel’s infrastructure be secured with basic security tools (anti-malware/virus software, firewalls, etc.).

6. In the event of a security incident, Gabriel reserves the right to request an audit of the third parties processes or methods leading to the incident.

7. Third party must report any known or suspected security-related incident to Gabriel immediately.