Information Security Policy

Confidential and Proprietary

Table of Contents

Introduction

Information management is a key component to an organization's success. GCommerce Inc.'s management has formed a set of information security policies and supporting procedures in accordance with regulatory industry security requirements.

Purpose

These polices and supporting procedures are designed to provide GCommerce Inc. with a documented and formalized set of standards to be adhered to and utilized throughout the organization at all times. Conformity with the stated policy and supporting procedures helps ensure the safety and security of all GCommerce information systems.

Scope

This policy and supporting procedures encompass all information systems that are owned, operated, maintained, and controlled by GCommerce Inc and all other information systems, both internally and externally, that interact with these systems.

- Internal information systems are those owned, operated, maintained, and controlled by GCommerce Inc. and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other information systems deemed in scope.

- External information systems are those owned, operated, maintained, and controlled by any entity other than GCommerce, but for which such external resources may impact the overall security of the description of "internal information systems".

Employees who undertake such measures are placing a high priority on the overall security of GCommerce Inc network, and in doing so, are promoting best practices for the organization.

Policy and Procedure Review

The policies, supporting procedures and appendixes are to be evaluated on an annual basis by the IT management team for ensuring its adequacy and relevancy regarding GCommerce's needs and goals. All changes to the policy and procedures will be documented, published, and communicated to all employees upon review and approval by Chief Technology Officer.

Note: If the information in an appendix is changed between review periods, the date and approval of changes contained in the appendix are noted on the appendix itself.

A Team Effort (Roles & Responsibilities)

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including management, internal employees and users of information systems, along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to GCommerce's information systems, all relevant parties are helping promote the security principles for information security in today's world of growing cybersecurity challenges.

Management Commitments

Responsibilities include providing overall direction, guidance, leadership and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations. The CTO is to

report to other members of senior management on a regular basis regarding all aspects of the organization's information systems posture.

Internal Employees and Users

Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any GCommerce information systems. Additionally, end users are to report instances of non-compliance to senior authorities, specifically those by other users. End users – while undertaking day-to-day operations – may also notice issues that could impede the safety and security of GCommerce information systems and are to also report such instances immediately to senior authorities.

Vendors, Contractors, Other Third-Party Entities

Responsibilities for such individuals and organizations are much like those stated for end users: adhering to the organization's information security policies, procedures, practices, and not undertaking any measures to alter such standards on any such information systems.

Access Management

Access rights to GCommerce Inc information systems are limited to authorized personnel only, with all end-users being properly provisioned in accordance with stated access rights policies and procedures. This includes using all applicable provisioning and de-provisioning procedures as necessary along with ensuring users access rights incorporate Role Based Access Control (RBAC) protocols or similar access control initiatives.

Additionally, users with elevated and/or super user privileges, such as system administrators, I.T. engineers and other applicable personnel, are responsible for ensuring access rights for all users (both end users and users with elevated and/or super user privileges) are commensurate with one's roles and responsibilities within GCommerce Inc.

The concepts of "separation of rights" and "least privileges" are to be adhered to at all times by GCommerce regarding access rights to information systems. Specifically, "separation of rights" implies that both the "functions" within a specified information system, for which there are many, should be separated along with the roles granted to end-users and administrators of these very information systems. "Functions" pertains to the actions an information system and its supporting components (i.e., the OS and applications residing on the server) can perform and the associated personnel who have authority over these functions. Thus, when permissible, functions (such as read, write, edit, etc.) should never be grouped together and end-users and administrators should not be granted access to multiple functions.

By effectively separating access rights to information systems whereby only authorized individuals have access to the minimum rights needed to perform their respective duties, GCommerce Inc is adhering to the concept of "least privileges", a well-known and best practices rule within information technology.

Furthermore, passwords used by all users must meet or exceed all stated GCommerce policies for password complexity requirements which can be found with the GCommerce Inc. Handbook.

Additionally, Access Management policy requires:

- All users are required to use their unique usernames for all activities.
- System admins have Domain Admin privileges, all other users have bare minimum credentials required to perform their work tasks to follow "least privileges".
- Users are added to Active Directory groups based on their roles.
- All Active Directory and Local user accounts are reviewed for removal bi-annually.
- Changes to an employee's access require management approval and can only be made at the request of approving management.

- Internal user access to the production environment is granted based on a specific need, and approval from the CTO.
- External vendors are assigned bare minimum permissions to do work as needed and removed from the system as soon as the need is satisfied.
- Vendors that must access the network do so after appropriate vetting and access our network via restrictive permissions and VPN connectivity.
- Remote sessions auto log-off after 2 hours of inactivity.

Information Flow Management

GCommerce uses Secured/Encrypted protocols for all cloud storage. These protocols include FTP, SFTP, AS2, and HTTPS/TLS to exchange documents between customers and various systems.

All requests made against the AWS and Azure storage accounts take place over secured connections and are only made from our internal systems.

- **Automated data encryption**—All data written into AWS and Azure Storage is encrypted by using Storage Service Encryption (SSE). This includes metadata.
- **Role-Based Access Control (RBAC)**—Roles with different permissions are assigned to resource groups storage accounts and individual containers.

Identity & Password Security Management

- Multi-factor authentication solution to comply with security mandates (MFA).
- Leveraging a mobile device or email to accept authentication requests (MFA).
- Passwords will be expired every 90 days and the user will be prompted to reset them via a secured channel.
- User identity is verified before performing password resets.
- Passwords will not be displayed when entered.
- Password complexity requirements include uppercase letters, lowercase letters, and a minimum password length.
- Passwords are changed whenever there is any indication of possible system or password compromise.

Access Logging/Monitoring

User activity and transactions are logged to identify unauthorized access and for debugging system errors. Every login attempt logs all the additional user information listed below:

- User ID and User Domain.
- Login failed or successful.
- User's browser version.
- The total activity times.
- Environment (e.g. environment variables, other settings, etc.) on application startup. This is helpful for debugging issues.
- All errors and warnings during the user activity.
- All metrics related to the Rest and SOAP APIs.

De-Provisioning Users

Terminating users (whether voluntary or involuntary) is a critical component of the user identity, provisioning, & access rights lifecycle, and as such, comprehensive measures are implemented for ensuring that all terminated users are appropriately removed from having access to any GCommerce information systems. Failure to enact these measures could potentially result in a breach of security for GCommerce as terminated users may still be able to gain authorized access to company-wide information systems. The following procedures to be undertaken include the following:

- Completing off boarding process within BambooHR and contacting via email, telephone or in person, all appropriate personnel responsible for terminating users from all company-wide information systems.

- Additionally, obtaining signatures on the applicable form from all individuals directly involved in the actual de-provisioning | off-boarding procedures for the terminated users.
- Confirming that system access to all company-wide information systems for terminated users has been effectively removed, which includes undertaking the following procedures:
    - Inspecting all information systems and supporting utilities for which authentication and authorization rights were initially established for terminated users.
    - Obtaining appropriate evidence (i.e., system screenshots and other system settings as necessary) from these information systems that terminated users were effectively removed from access and attaching the applicable documentation to a specified user de-provisioning form.

Critical accounts for terminated users are to be appropriately maintained by authorized personnel for ensuring that correspondence, such as emails and voicemails are addressed in a timely manner by GCommerce. As such, the following critical accounts are to be monitored following the de-provisioning | off-boarding process for terminated users:

- Email Accounts
- Voice Mail

All exceptions for de-provisioning users must be clearly documented within the procedures document.

Administration & Maintenance

- Notifications to Admins when accounts are no longer needed.
- Administer access authorizations and privileges are in accordance with access and functional requirement.
- Modifying or removing system access when the assignment, job responsibility, or business requirement for access changes or is no longer needed.
- Deactivating and deleting accounts that are no longer required, and accounts of terminated or transferred users.
- Ensuring that user accounts are automatically locked for 3 consecutive unsuccessful login attempts.
- Terminating Remote Access based on account terminations and IT needs.

System Monitoring

Effective protocols and supporting measures are to be implemented for ensuring all required events and their associated attributes are logged, recorded, and reviewed as necessary. Additionally, all applicable elevated permissions (those for administrators) along with general access rights permissions (those for end-users) to GCommerce Inc information systems are to be reviewed on a bi-annual basis by an authority that is independent from all known users (i.e., end-users, administrator, etc.) and who also has the ability to understand, interpret, and ultimately identify any issues or concerns from the related output (i.e., log reports, and other supporting data). The specified authority reviewing the logs is to determine what constitutes any "issues or concerns", and to report them immediately to appropriate personnel.

Moreover, protocols such as syslog and other capturing and forwarding protocols and, or technology, such as specialized software applications, are to be used as necessary, along with employing security measures that protect the confidentiality, integrity, and availability (CIA) of the audit trails and their respective log reports (i.e., audit records) that are produced. Additionally, all audit records are to be stored on an external log server (i.e., centralized syslog server or similar platform) that is physically separated from the original data source, along with employing effective backup and archival procedures for the log server itself. These measures allow GCommerce Inc to secure the audit records as required for various legal and regulatory compliance mandates, along with conducting forensic investigative procedures if necessary.

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified, as appropriate, for changes in conditions. Management and key personnel are responsible for monitoring the quality of the internal control environment as a regular part of their activities. GCommerce utilizes an independent 3rd party (Pratum) to perform vulnerability scanning and penetration testing to test the effectiveness and efficiency of the control environment for the Commerce Bridge system. Independent security assessments and audits are performed on a recurring basis to ensure controls are updated and modified, as necessary.

GCommerce also utilizes a managed security services provider ("MSSP") to provide SIEM services. Alerts are generated and reviewed at the MSSP for suspicious critical activity and security tickets are opened and an IT team member is notified of the potential issue. The IT team member will then investigate and, if necessary, remediate the issue and provide resolution details to the MSSP so the security ticket can be updated and closed for tracking and reporting purposes. A monthly meeting is held with the MSSP to review reports, ticket status, and current configurations.

GCommerce uses Nagios to monitor, alert and report on all systems and services. Metrics monitored include Availability, UpTime, CPU / MEM / Network / Disk utilization and rate, extra SQL metrics, IIS metrics, and system logs for supported systems. Uptime Robot is also utilized to monitor our external-facing services from offsite to ensure public access to our services.

We utilize a 3rd party hosted SIEM for log forwarding, monitoring and alerting. Our Cisco FirePower router utilizes the latest IPS and Threat Response tactics and works in concert with our Cisco AMP endpoint protection, all backed by Cisco Talos Threat Intelligence. GCommerce undergoes annual port scans and is alerted by our SIEM provider of any unknown access to any of our infrastructure. We use SalesForce.com for our CRM and our ticket management system. Tickets are entered manually on an as-needed basis and are assigned to the appropriate technician for that product and closed when resolved. Communication with clients includes email and phone calls as needed on a per-incident basis.

Audit Logs

This policy provides guidelines for the appropriate use of auditing and logging in computer systems, networks, and other devices that store or transport critical and/or security-sensitive data.

Activities to be Logged

Therefore, logs shall be created whenever any of the following activities are requested to be performed by the system:

1. Create, read, update, or delete confidential information, including confidential authentication information such as passwords;
2. Create, update, or delete information not covered in #1;
3. Initiate a network connection;
4. Accept a network connection;
5. User authentication and authorization for activities covered in #1 or #2 such as user login and logout;
6. Grant, modify, or revoke access rights, including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall rules, and user password changes;
7. System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes;
8. Application process startup, shutdown, or restart;
9. Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources), the failure of network services such as DHCP or DNS, or hardware fault; and

10. Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

Elements of the Log

Such logs shall identify or contain at least the following elements, directly or indirectly. In this context, the term "indirectly" means unambiguously inferred.

1. Type of action – examples include authorize, create, read, update, delete, and accept network connection.
2. Subsystem performing the action – examples include process or transaction name, process or transaction identifier.
3. Identifiers (as many as available) for the subject requesting the action – examples include user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
4. Identifiers (as many as available) for the object the action was performed on – examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized in order to facilitate log correlation.
5. Before and after values when action involves updating a data element, if feasible.
6. Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time.
7. Whether the action was allowed or denied by access-control mechanisms.
8. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

Formatting and Storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs and to support enterprise-level analysis and reporting. Note that the construction of an actual enterprise-level log management mechanism is outside the scope of this document. Mechanisms known to support these goals include but are not limited to the following:

1. Microsoft Windows Event Logs collected by a centralized log management system;
2. Logs in a well-documented format sent via syslog, syslog-ng, or syslog-reliable network protocols to a centralized log management system;
3. Logs stored in an ANSI-SQL database that itself generates audit logs in compliance with the requirements of this document; and
4. Other open logging mechanisms supporting the above requirements including those based on CheckPoint OpSec, ArcSight CEF, and IDMEF.

Business Continuity and Disaster Recovery

Documented Business Continuity and Disaster Recovery Planning (BCDRP) initiative is vital to protecting all GCommerce Inc assets along with ensuring rapid resumption of critical services in a timely manner. It is the responsibility of authorized GCommerce personnel to have in place a fully functioning BCDRP process, and one that also includes specific policies, procedures, and supporting initiatives relating to all information systems.

Business Continuity and Disaster Recovery ("BC/DR") Plan is to guide the business in the case of a disaster or disruption to ensure rapid resumption of critical services in a timely manner. GCommerce's Business Continuity and Disaster Recovery Plan leverages a risk-based analysis (from the Risk Assessment) that also includes specific policies, procedures, and supporting initiatives relating to all information systems.

Refer to the Business Continuity Management Policy and Disaster Recovery Plan for more details.

Data Governance

Data Categorization

All data except for company financial, corporate and technical documentation is classified equally as moderate to low security. This means all internal staff can view and work with customer data but cannot share this data outside our organization or approved authorized contractors without customer consent.

In addition, data and information being stored, processed, and/or transmitted on information systems that are owned, operated, maintained and controlled by GCommerce Inc are to have appropriate classification levels in place that consist of the following:

- **Unclassified | Public Information:** This type of data and information, and the underlying information assets associated with it, is generally designed to be used by anonymous individuals or systems that have a credible interest in communicating with GCommerce Inc As such, this type of data and information is disclosed freely to the general public.
- **Proprietary:** This type of data and information, and the underlying information assets associated with it, is generally designed to be used by internal employees only, thus it is prohibited from being circulated outside of the organization.
- **Confidential:** This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by select employees only.
- **Company Confidential:** This type of data and information must be protected from unauthorized access at all times, but with a focus on the data and information being that of internal, corporate issues.
- **Client Confidential:** This type of data and information must be protected from unauthorized access at all times, but with a focus on the data and information being that of the customers.
- **Sensitive:** This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by very select employees only. Furthermore, it requires an extremely high level of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).
- **Trade Secret:** This type of data and information, and the underlying information assets associated with it, is also intended to be viewed and/or utilized by very select employees only. Furthermore, it too requires an extremely high level of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).
- **Top Secret:** This type of data and information, and the underlying information assets associated with it, is intended to be viewed and/or utilized by an extremely select number of employees only. Furthermore, it requires the highest levels of protection from unauthorized parties for ensuring its confidentiality, integrity, and availability (CIA).

Data Retention

It is company policy to limit data storage amount and retention time to that which is required for legal, regulatory and business requirements. Furthermore, processes are in place for secure disposal of data when no longer needed for legal, regulatory, and business requirements. This in turn mandates retention requirements and documented accordingly for all legal, regulatory, and business requirements. Additionally, an automatic or manually executed process is to be in place for identifying and securely removing data that exceeds the defined legal, regulatory and business requirements. As for disposing of data, the following methods are to be utilized for both hard copy and electronic data:

- Purging and deleting data from all information systems. This can be done by utilizing a secure wipe program in accordance with industry-accepted standards for secure deletion (i.e., degaussing).
- Destroying (cross-shredding) any cardholder data that is in a hardcopy format.

For electronic media stored on information systems that are no longer in use, data is to be disposed of through any one of the following procedures:

- Disintegration
- Shredding (disk grinding device)
- Pulverization

Data Backup and Recovery

GCommerce uses VEEAM backup and recovery for data recovery and individual system recovery, utilizing backup to disk, then copy to tape, and backup to Azure for offsite storage. Full backups run weekly and Incremental Backups run nightly. Network Admins monitor the backup software and remediate any failures as need. Additionally, we use Azure Site Recovery to maintain a DR site for catastrophic failover.

The Commerce Bridge platform is secured using AV/AM as well as AR software. For AV endpoint protection we use Cisco AMP which is also integrated with our Firepower Cisco Firewall appliance for a complete platform protected solution. For AM we use Malwarebytes with AR, anti-ransomware. Both Cisco AMP and Malwarebytes are managed through a common administrator portal where we review the products' status and take corrective action if necessary.

Data Security Breaches

Data security breaches whether defined as the intentional or unintentional release of secure information into an untrusted environment. Employees must understand and help to protect the safety and security of organizational-wide information systems. As a GCommerce Inc. employee, you will come across information deemed highly sensitive and confidential, so remember to ask yourself some basic questions, such as "Do I have the right to access this information, is the information being stored securely from unauthorized parties", and many other basic security questions. It's also important to note the different types of data security breaches, which - according to privacyrights.org - generally consist of the following:

- **Unintended disclosure** - Sensitive information posted publicly on a website, mishandled or sent to the wrong party via email or any other type of end-user messaging technology.
- **Hacking or malware** - Electronic entry by an outside party, malware and spyware.
- **Payment Card Fraud** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- **Insider** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
- **Physical loss** - Lost, discarded or stolen non-electronic records, such as paper documents
- **Portable device** - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape, etc.
- **Stationary device** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
- **Unknown** - Anything outside of the above listed categories.

Our reliance on information technology - though plentiful with benefits - also brings large risks and even larger responsibilities by employees for being aware of any perceived or actual instances of intentional or unintentional release of secure information into an untrusted environment. Data security breaches are costly, extremely damaging, with long-lasting negative effects. Again, if you see something, say something - immediately!

Refer to Incident Response Plan for all actions required for an incident.

Encryption Requirements

When necessary and applicable, appropriate encryption measures are to be invoked for ensuring the confidentiality, integrity, and availability (CIA) of GCommerce Inc information systems and any sensitive data associated with it. Additionally, any passwords used for accessing and/or authentication to the specified information systems are to be encrypted at all times, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such as Secure Sockets Layer (SSL) | Transport Layer Security (TLS), Secure Shell (SSH), and many other secure data encryption protocols are to be utilized when accessing the specified information systems. Additional encryption measures for GCommerce Inc are to also include the following best practices for all applicable devices that have the ability to store sensitive and confidential information:

- **Servers -** Use the industry standard AES-256 encryption algorithm to encrypt data on the server. Depending on the type of server and the underlying applications, a large range of encryption measures can be adopted. The first measure is identifying the type of information residing on such servers and the necessary encryption protocols to apply. Additionally, servers are to be provisioned and hardened accordingly, with anti-virus also installed.
- **Desktop Computers -** Any desktop computer storing sensitive and confidential information are to utilize encryption for the actual hard drives. Additionally, access rights are to be limited to authorized personnel at all times. Non-company owned desktops, such as those physically located at an employee's home, are to never contain sensitive and confidential information under any circumstances. If such data needs to be accessed for performing remote duties, then a secure connection must be made to the GCommerce Inc network for accessing all relevant information. Additionally, desktop computers are to be provisioned and hardened accordingly, with anti-virus also installed.
- **Laptops, Mobile Computing Devices, Smart Devices -** Such devices are to have approved encryption installed and enabled prior to their use, which requires GCommerce Inc authorized I.T. personnel to configure appropriate encryption programs. If such data needs to be accessed for performing remote duties, then a secure connection over VPN must be made to the GCommerce Inc network for accessing all relevant information. Additionally, laptops, mobile computing devices, and smart devices are to be provisioned and hardened accordingly, with anti-virus also installed.
- **Removable Storage Devices -** USB enabled devices, such as memory sticks, external hard drives, network attached storage devices are strictly prohibited. Though there may be circumstances that require storing of sensitive and confidential information onto these utilities, it must be approved in writing, and such data is never to reside on these devices for long-term storage measures.
- **Databases -** use the industry standard AES-256 encryption algorithm to encrypt data DB instances.

Asset Management

The success of one's overall information security initiatives is highly dependent on identifying all relevant information systems, which ultimately entails having a comprehensive asset inventory list in place. As such, GCommerce Inc is to identify all applicable unique identifiers and necessary data elements for successfully tracking and managing such an inventory. At a minimum, the following elements are to be used for asset inventory, when applicable:

- Type of information systems – Network devices (firewalls, routers, switches, load balancers, etc.)
- Type of information systems – Servers (physical and or/logical, and the underlying operating systems and applications residing on such servers).
- Primary function.
- Physical element: A stand-alone product, or a virtual element, such as an instance, etc.

- Internal hostname.
- Physical location.

Computer Provisioning and Baseline Hardening Policy

All GCommerce Inc information systems are to be properly provisioned, hardened, secured, and locked-down for ensuring their confidentiality, integrity, and availability (CIA). Improperly or poorly provisioned systems can often result in network exploitation by hackers, malicious individuals, and numerous other external, and internal threats. Therefore, the following provisioning and hardening procedures are to be applied as necessary when deploying information systems onto GCommerce Inc 's network:

- Vendor-supplied default settings are changed.
- All unnecessary accounts are eliminated.
- Only necessary and secure services, protocols and other essential ports are enabled as needed for functionality.
- All unnecessary functionality is effectively removed.
- All system security parameters are appropriately configured.
- Documented system configuration standards are applied via documented provisioning and hardening checklists.

Provisioning and hardening all GCommerce Inc information systems greatly increases their overall security in that insecure services that were effectively removed and/or disabled now cannot be used to attack and ultimately compromise such I.T. resources. Additionally, the fewer the number of services and protocols in use, the greater the chances of interoperability and compatibility with other information systems, both internally and externally. Furthermore, one's ability to comprehensively review and detect issues or concerns from information systems log reports is much greater when only necessary services or protocols are enabled, rather than a myriad of settings that produces voluminous audit trails, which can be challenging to monitor.
Regarding provisioning and hardening, this critical and time-consuming process is to be undertaken by authorized personnel only; a select number of individuals who have the authority and applicable skill-sets to conduct these activities.

Anti-Virus/Anti-Malware

Malicious software (malware) poses a critical security threat to GCommerce Inc information systems, thus effective measures are to be in place for ensuring protection against viruses, worms, spyware, adware, rootkits, trojan horses, and many other forms of harmful code and scripts. As such, GCommerce Inc is to have anti-virus (AV) solutions deployed on all applicable information systems, with the respective AV being the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans as necessary. Because strong and comprehensive malware measures are not just limited to the use of AV, additional tools are to be employed as necessary for eliminating all other associated threats, such as those discussed above. The seriousness of malware and its growing frequency of attacks within organizations require that all I.T. personnel within GCommerce Inc stay abreast of useful tools and programs that are beneficial in combating harmful code and scripts.

Firewall Configuration Policy

Firewall configurations are reviewed by management frequently to ensure all established rules have business justification and unnecessary rules are removed timely. Replacement rules are created and tested inappropriate rules and implemented, as appropriate.

Securing and Updating Systems

While I.T. professionals are busying updating and applying critical security patches to GCommerce Inc information systems, it's important that all employees also do the same for many of their devices, particularly applications used

on a daily basis. Security is the first and foremost reason for applying security updates, but there are other benefits also, such as new and enhanced features, improved performance and stability. Additionally, security updates are almost always free - so there's another compelling reason! Along with ensuring that a current and stable version of anti-virus is being used, the following are to be updated accordingly:

- Internet browsers: Updating browsers (Internet Explorer, Mozilla, Google Chrome) is extremely important for ensuring all web pages display correctly, security holes are not still present, and all performance features are maximized.
- Microsoft Windows Operating Systems: GCommerce has regular managed updates and are pushed out on a regular basis.

Other essential applications: There's an almost endless list of applications being used today, so keep a list handy of what's on your computer, making sure to perform security updates as required for not only safety, but performance and software stability.

Network Security

Network Access/Configuration Policy

GCommerce Inc has established the following general guidelines, responsibilities, and acceptable uses for network devices as described below.

- All network devices are to be configured and used strictly for business operations.
- All network devices are to be appropriately hardened and secured in accordance with industry standards and for applicable business requirements.
- Any network devices obtained without proof of purchase and licensing rights will not be allowed onto the network.
- All users (primarily system administrative users) must be responsible for the proper use of these devices.
- Any activity that may potentially compromise the organization’s network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization because of misuse of these devices will not be tolerated.
- All network system administrative rights and subsequent activities undertaken on network devices are subject to audit and review as needed.
- Users are to have their access rights permanently revoked from all computing systems that allow for access to any network devices once they have been terminated. This includes the disabling of email accounts and passwords for any user terminated by GCommerce Inc Terminated users will not be allowed to have any e-mails forwarded to them once they have been terminated.

The following activities are considered **unacceptable** by users.

- Any activity resulting from the use of GCommerce Inc network devices that may potentially compromise the organization’s network infrastructure, cause harm to other related systems, cause harm or pose a significant financial, operational, or business threat to the organization because of inappropriate and unacceptable use of network devices.
- Users are strictly prohibited from utilizing GCommerce Inc network devices for the purposes of connecting to and viewing any sites with explicit sexual content (minor or adult), racist content, sites that invoke terroristic material, promote violence, along with any other offensive material and any other content deemed unprofessional, unethical or that violates any local, state, or federal law or regulation.
- Users are strictly prohibited from utilizing network devices for the purposes of engaging in any type of illegal activity that violates any local, state, or federal law or regulation.

- Users are strictly prohibited from utilizing GCommerce Inc network devices for discussing confidential and sensitive company information with unapproved third-party entities. This confidential and sensitive information, may include, but is not limited to, the following: trade secrets, patents, financial, operational, or technology data.
- Users are only allowed to access their own respective network devices they are assigned to and are strictly prohibited from accessing another employee's network devices. Additionally, modifying network devices regarding system settings without documented approval and business justification is strictly prohibited.
- Network components may not be added, removed or modified unless explicit consent is given by appropriate personnel.

Network and Server Patching Essentials

All necessary system patches and system updates to GCommerce Inc information systems (those defined as critical from a security perspective) are to be obtained and deployed in a timely manner. Effective patch management and system updates help ensure the confidentiality, integrity, and availability (CIA) of systems from new exploits, vulnerabilities and other security threats.

Various external security sources and resources are to be utilized for ensuring that GCommerce Inc maintains awareness of security threats, vulnerabilities and what respective patches, security upgrades and protocols are available. Authorized I.T. personnel are to subscribe to the following types of security sources and resources for ensuring retrieval of security patches in a timely manner:

- Vendor websites and email alerts, such as those for Microsoft, UNIX, Linux, Cisco, HP, etc.
- Vendor mailing lists, newsletters and additional support channels for patches and security
- Approved third-party websites, email alerts, and mailing lists
- Approved online information security forums and discussion panels
- Information security conferences, seminars and trade shows

Network Time Protocol

Correct, accurate and consistent time on all GCommerce Inc information systems entail procedures for properly acquiring, distributing and storing time from industry accepted external sources; those which are based on Coordinated Universal Time (UTC), which is essentially based on International Atomic Time (TAI). And while there are several protocols to synchronize computer clocks, Network Time Protocol (NTP) is highly favored by GCommerce Inc as it requires a reference clock for defining true and accurate time, is fault-tolerant, highly-scalable, and uses trusted external sources (such as UTC). Moreover, NTP's hierarchical structure of clocks, where each level is termed a "stratum", has proven to be a trusted and reliable source for time synchronization. And because the Windows Time Service is not considered to be an accurate measurement of time, other time synchronization technologies are to be implemented.

Cloud Computing Essentials

It's also critical that employees have a strong understanding of cloud computing, which is an area within information security that contains an almost endless list of definitions and explanations, ranging from the very technical (NIST definition of cloud computing), to the more-simpler, and easy-to-understand definition.

The following pertains to all cloud services used within GCommerce:

- Use of cloud computing services for work purposes must be formally authorized by the CTO. The CTO will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.
- For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the IT Manager/CIO.
- The use of such services must comply with GCommerce's existing Acceptable Use Policy/Computer Usage Policy/Internet Usage Policy/BYOD Policy.

- Employees must not share log-in credentials with co-workers. The IT department will keep a confidential document containing account information for business continuity purposes.
- The use of such services must comply with all laws and regulations governing the handling of personally identifiable information, corporate financial data or any other data owned or collected by GCommerce Inc.
- The CTO decides what data may or may not be stored in the Cloud.
- Personal cloud services accounts may not be used for the storage, manipulation or exchange of company-related communications or company-owned data.

Change Management

GCommerce follows a structured change management process for application development, which is documented within the Company's Product Round Table (PRT) process and Project Life Cycle (Change Management) Process standards. This standard provides structure and consistency for a successful software project.
All requests (changes, enhancements, new products) originate from one of the three sources below:

- Direct Customer requests
- Enhancement requests from internal resources to help them save time/effort
- Enhancement requests from internal resources – that are raised to improve the existing system or to fulfill the "expected behavior" of the existing system

Refer to the Project Life Cycle (Change Management) Process document for details.

Systems Development

The Project Life Cycle (PLC) for GCommerce Inc is to encompass a number of phases, each concluding with a major milestone. Assessments are conducted after each phase to determine if objectives have been satisfied. Throughout these phases within the Project Life Cycle, all personnel involved are to be collaborating to engage the business to actively participate which will help requirements to evolve throughout the project to ensure the work being done is the right product. All activities for internally developed systems/applications and projects are to consist of the following procedures and phases:

- **Project Initiation/Project Prioritization** - The initiation phase aims to define, authorize and prioritize the project. The project manager/scrum master presents the Project requests to the PRT committee. The PRT committee authorizes the project and identifies the primary requirements for the project.
- **Requirements** – Business Analysts will define the requirements for the iteration based on the product backlog, iteration backlog, customer and stakeholder feedback. Requirements are written as user stories from the user's perspective.
- **Development** – Application Developers will design and develop software based on defined requirements.
- **Testing** – Application Tester will write test cases and Quality Assurance (QA) testing on defined requirements.
- **Training/Documentation development** – Business Analysts in collaboration with the Customer Support team will create documentation for internal and external training. Internal training will be completed by the Business Analyst and external user training will be completed by the Customer Support team.
- **Release for Production** – Once the system/application, feature or tool is successful in the test environment, GCommerce approves the release for production. Technical Lead will move modules to the production servers where functionality is tested after all modules are updated.
- **Delivery** – Implementation team/Specialist will integrate and deliver the working iteration into production.
- **Feedback** – Implementation team and Sales team will take customer and stakeholder feedback and work it into the next project requests review.

Configuration Management Policy

Because configuration management and its overall application often vary throughout industries and business sectors, for scope purposes, GCommerce Inc defines such practices as those utilized for implementing, establishing, maintaining, recording, and effectively monitoring secure configurations to the organization's overall information systems landscape. Specifically, this includes all network devices, operating systems, applications, internally developed software and systems, and other relevant hardware and software platforms. If any specific systems, because of size or complexity challenges, ultimately require their own independent configuration management program, they are to be developed accordingly by authorized personnel, and must abide by the practices as stated herein. Additional provisions for configuration management also include the following:

- Appropriate roles and responsibilities are to be developed and subsequently assigned to authorized personnel within GCommerce Inc regarding configuration management practices.
- All employees and relevant users of GCommerce Inc information systems are to receive the required and necessary training for undertaking their roles and responsibilities for configuration management. Training varies by personnel, but is to include all measures for ensuring employees and users stay abreast of significant issues affecting configuration management.
- Authorized personnel are to identify, assess, and select specific software tools and related utilities for aiding and facilitating all aspects of GCommerce Inc 's configuration management plan. This entails extensive research into all possible configuration management tools for ensuring interoperability and compatibility with all in-scope information systems, while also ensuring such tools have appropriate end-user technical and operational support at all times.
- Authorized I.T. personnel are to determine a variety of factors, most importantly the following: The minimum agreed upon security settings for ensuring a risk level as low as possible, yet one that still allows the organization to function in an efficient and effective manner, from an operational perspective.
- Authorized I.T. personnel are to identify baseline configuration standards for information systems, which are available from a number of well-known benchmarks, frameworks, associations, along with vendor specific guides.
- For all in-scope information systems, insecure services, ports, and protocols are to be readily identified by authorized I.T. personnel, which means having a strong technical understanding of all relevant network devices (i.e., firewalls, routers, switches, load balancers, etc.), operation systems (i.e. Windows, UNIX, Linux), and applications (i.e., file server applications, web server applications, database applications).

Vulnerability Management

An essential component of any vulnerability management program is to comprehensively identify and define the security posture of the organization as a whole. Increasing cyber security threats, regulatory compliance mandates, the implementation of best practices, and other important operational and security considerations are to be identified when defining such a posture. Ultimately, a well-conceived vulnerability management program for GCommerce Inc is one that ensures the confidentiality, integrity, and availability (CIA) of the organization's information systems landscape, which includes all critical information systems. Vulnerability management programs – often confined to only conducting internal and external scans, along with penetration testing, and remediating such issues – is to also include identifying and detecting, classifying and prioritizing, remediating, validating, and continuously monitoring vulnerabilities relating to the following:

- **User Access Rights:** Ensuring users have access rights commensurate to one's roles and responsibilities within the organization is a constant challenge, given the continuous user provisioning and de-provisioning processes undertaken, the numerous systems requiring access for such users, along with requests for changes and modifications in access rights.

- **Configuration Standards:** Provisioning, hardening, securing and locking-down all critical information systems within GCommerce Inc is crucial for ensuring a baseline of information security, one that can be built upon over time by continuous monitoring and updating of such systems with security patches.
- **Network Architecture and Topology:** Insecure network topologies and weak security architectures – even if the systems themselves are properly secured and hardened – can result in significant vulnerabilities for the organization.
- **Network Vulnerabilities:** The use of internal and external vulnerability scanning procedures, along with network layer and application layer penetration tests are a critical component of GCommerce Inc 's vulnerability management program.

Ultimately, an important component of developing a comprehensive vulnerability management program requires GCommerce Inc to adequately address the following major issues and constraints:

- **Vulnerabilities:** Software flaws or a misconfiguration that may potentially result in the weakness in the security of a system within the organization's information systems.
- **Remediation:** The three (3) primary methods of remediation are (1) installation of a software patch, (2) adjustment of a configuration setting and (3) removal of affected software.
- **Threats:** Threats are capabilities or methods of attack developed by malicious entities to exploit vulnerabilities and potentially cause harm to a computer system or network.

Penetration Tests and Vulnerability Scans

All applicable GCommerce Inc information systems are to undergo annual vulnerability assessments along with penetration testing for ensuring their safety and security from the large and ever-growing external and internal security threats being faced with today. Vulnerability assessments, which entails scanning a specified set of network devices, hosts, and their corresponding Internet Protocol (IP) addresses, helps identify security weaknesses within GCommerce Inc 's network architecture, along with those related to specific information systems. Additionally, penetration testing services, which are designed to actually compromise the organization's network and application layers, also assists in finding security flaws that require immediate remediation. Moreover, contractual requirements along with regulatory compliance laws and legislation often mandate organizations perform such services, at a minimum, annually (for penetration tests), and often on a periodic and/or quarterly basis (for vulnerability assessments). As such, GCommerce Inc will adhere to these stated requirements and will perform the necessary services on all applicable information systems.

Careful planning and consideration of what systems are to be included when performing vulnerability assessments and, particularly penetration testing, is a critical factor, as all environments (i.e., development, production, etc.) must be safeguarded from any accidental or unintended exploits caused by the tester.
Additionally, if GCommerce Inc has internally developed, proprietary applications (i.e., software), appropriate code reviews are to be conducted for ensuring the software itself has been coded and developed with the relevant security measures. Poorly coded software, specifically software used for web facing platforms, can be compromised through numerous harmful tactics, such as Cross-site scripting (XSS), injection flaws (SQL, etc.) and other damaging methods.

Wireless Environments

Initially implementing a WLAN requires adherence to the following stated guidelines for ensuring the safety and security of the wireless platform itself, along with ensuring the confidentiality, integrity, and availability (CIA) of GCommerce Inc 's overall information systems landscape:

- **Secure Deployment:** All WLAN devices and supporting resources, such as wireless access points, and other network devices, are to be positioned in a manner for ensuring unauthorized physical access and modification. Additionally, they are to be secured with approved fixtures and other necessary apparatuses

for mitigating any unnecessary movement. Additionally, the WLAN platform itself is to be logically | physically segregated from the corporate | internal wired network, which can be achieved by utilizing firewalls and other access control methods.

- **Asset Inventory:** Once all WLAN devices are safely secured, a complete asset inventory is to be taken, documenting all necessary information, such as physical location, and corresponding unique identifiers (i.e., hostnames, serial numbers, etc.).

- **Configuration of Wireless Access Points:** The following measures are to be undertaken regarding WLAN platforms:

    - Change default administrator settings, such as username and password, along with implementing strong, unique administrative passwords (i.e., alphanumeric, case sensitive, etc.) for all wireless access points.
    - Change any default IP addresses also.
    - Configure SNMP and NTP accordingly.
    - Configure wireless modes to support only the one (1) primary - and industry approved - wireless networking standard.
    - Change vendor default settings for Service Set Identifier (SSID) to a completely new network name, but also one that does not openly identify or provide any critical [company] name information. Specifically, the SSID character string is not to reflect company name.
    - Use a "closed network" concept, whereby the SSID is actually not broadcasted (if allowable), rather, it must be entered into the client application.
    - If the SSID must be broadcasted, create a healthy balance of allowing all authorized users to receive such signals, but not the point where unauthorized parties can potentially view such information.
    - Remove all unnecessary and insecure services and protocols from all WLAN devices, such as the wireless access points and any all other associated wired network devices.
    - For all remaining services and protocols, implement the concept of "least privileges".
    - Implement MAC Address filtering and wireless access points.
    - Use the strongest encryption algorithm currently available (WPA2), and use other forms of encryption as needed, such as VPN, SSL | TLS, etc.
    - Protect all sensitive wireless access points information, such as administrator passwords, SSID password, keys, etc. with approved security measures, such as encryption itself.
    - Enable logging features and ensure that all logs and audit trails are sent to a remote logging server and retained as necessary (i.e., regulatory compliance laws, etc.). Information captured should include, but not limited to, the following: source\destination IP addresses, MAC addresses, user logon information (i.e., time, username, etc.), user logoff information.
    - Enable usage parameters, such as time-out sessions.
    - Disable wireless access points during non-business hours, such as nights, weekends, holidays, etc.

Risk Management

The core component of the information security program is identifying and managing risks to the organization and its business functions through the risk assessment and evaluation process. To support this core requirement, risks shall be assessed and tracked through a comprehensive set of actions. Identified risks shall either be avoided, controlled/mitigated, transferred, or accepted. If accepted, a specific risk acceptance procedure shall be used.

Risk Assessment and Tracking

Risk management is a key foundation of the information security program. As such, GCommerce Inc. will implement and maintain an on-going risk assessment program to determine risks to the organization. To be effective, this program shall include four key actionable components:

1. Evaluating and prioritizing assets;
2. Continually identifying vulnerabilities through multiple methods, such as internal research, vendor support sites, and testing (e.g., vulnerability scans, penetration testing, social engineering);
3. Staying current on the latest (potential) threats to the organization, such as through media/news threat information sharing forums, applicable laws and regulatory requirements; and
4. Estimating the likelihood of those threats exploiting or taking action against the organization.

Collectively, these actions will support leadership's ability to make informed decisions about risks and appropriate controls. A listing of IT/information security risks and controls will be maintained and routinely reviewed as part of the ongoing risk management process.

Risk Acceptance

Changes to information and information systems, if likely to introduce additional risk, will be evaluated prior to implementation. Risks to the organization's information and information systems shall be documented, tracked, and updated periodically. When risk is to be accepted, an approved risk acceptance procedure shall be used, including documenting the risk and management's approval/acceptance of that risk.

Third Party Risk Management

When external information system services are used, the service provider shall be required to comply with GCommerce's information security requirements and employ appropriate controls in accordance with contractual requirements, regulatory and compliance requirements, and applicable policies, standards, etc. Service delivery oversight and management roles and responsibilities shall be clearly defined and documented. Third-party service delivery shall be periodically audited and reviewed to monitor compliance with contractual and other applicable requirements. Significant changes (or potential changes) at the third-party provider, such as a merger or acquisition, may have impact on the provider's ability to effectively deliver on the requirements, and risks associated with third-party provider shall be periodically reviewed as part of the vendor management and risk management processes.

This will enable the Company, when appropriate, to:

- Classify third parties as high/critical, medium, or low depending on the risk to the company.
- Identify and manage/mitigate existing or potential risks associated with a third party that could adversely affect the Company and its operations;
- Evaluate the overall integrity and effectiveness of the third party's information security and risk management systems and controls;
- Determine compliance with applicable laws or regulations that affect the services provided by the third party;
- Facilitate an overall program that manages third party relationships;
- Properly perform due diligence and risk assessment when creating and maintaining a relationship with a third party based on the third party's risk to the Company and its customers;
- Provide for the review and negotiation of written contracts and/or service level agreements;
- Communicate third party exceptions and deficiencies to Management level committees and the Audit Committee;
- Monitor any significant changes in a third party's products, services, stability, or risk management practices that would adversely affect the Company; and
- Centralize the management and reporting of the implementation of this Policy.

The company will conduct an Information Security risk assessment on new and existing third parties. All third parties will be assigned an inherent risk classification based on the following:

Classification	Description	Frequency of Review
Critical/High Rating	• Processes, stores, hosts, or transmits restricted/confidential Data on behalf of client. • Has direct network access into client infrastructure. • Deemed mission critical and loss of third party will result in severe adverse impact.	At least annually and/or upon change in terms of services or contracts.
Medium Rating	• Has access to restricted/confidential data but does not process, store, hosts or transmit that data • Loss of third party will be tolerable, with moderate difficulty of replacement.	Every two (2) years and/or upon change in terms of services or contracts.
Low Rating	• Used for service enhancements but doesn't direct access to restricted/confidential data • Loss of third party will have low impact, replacement readily available.	Every three (3) years and/or upon change in terms of services or contracts.

Policies relating to Information Security in GCommerce Handbook and Acceptable Use Policy

The following policies and procedures can be found within the GCommerce Inc. Handbook and/or Acceptable Use Policy:

- BYOD Policy
- Cyber Security Awareness, Training, and Education
- Email Policy
- Internet Usage Policy
- Removable Storage Policy
- Password Policy
- Physical and Environmental Security Policies
    - Physical Security Measures
    - Employee Premise Access Policy
    - Visitor Premise Access Policy
    - Clean Desk Policy
    - Securing Workstations
- Remote User Access
- Social Media Policy
- Software Use

Review and Change History

This document will be reviewed annually and whenever there is a significant change to the business, to ensure continual alignment with the current needs of the organization.

Date	By	Action	Description	Approval Date	Approver Name & Role
3/25/2020	Diana Calo	Reviewed and Combined	Reviewed and combined multiple policies into one ISP document.	3/25/2020	Jason Popillion, CTO
4/13/2020	Ben Hall	Changed	Added Risk Management Policy	4/13/2020	Jason Popillion, CTO
4/15/2020	Diana Calo	Update	Added Third Party Risk Management Added encryption requirements in Data Governance Section Updated Network Security Section	6/21/2021	Jason Popillion, CTO/CIO