Grantd Equity, Inc.

StockOpter Application
Data Security and Privacy Policies Handbook

April 2026

Table of Contents

DATA SECURITY POLICY 4

In General 4
Information Security Organization 4
Data Security 4
Software Development 5
Access Management, Entitlement and Password Policies 5
Backups 6
Disaster recovery 6
Security Incident Policy 6
Outside contractors 6
Network security 6
Change Control / Change Management 7
Data Transfer and Decommissioning 7
Physical Site Security 7
Security Awareness Program 7
Asset classification and handling 8
PC and Server Security 8
Other Policies 8
Enforcement 9
Employee/Contractor Acknowledgement: 9
Employer Acknowledgement: 9
Appendix A – Security Access Warning Message 10

IT SECURITY POLICIES AND PROCEDURES - INFORMATION SENSITIVITY POLICY 11

Purpose 11
Scope 11
Protection Level by Security Class 12
Enforcement 12
Terms & Definitions 12
Revision History 13

IT SECURITY POLICIES AND PROCEDURES - ACCEPTABLE USE POLICY 15

1.0 Overview 15
2.0 Purpose 15
3.0 Scope 15
4.0 Policy 15
4.1 General Use and Ownership 15
4.2 Security and Proprietary Information 16
4.3. Unacceptable Use 16
4.4. Email and Communications Activities 18
4.5. Blogging 18
5.0 Enforcement 19
6.0 Definitions 19
7.0 Revision History 19

ACCEPTABLE ENCRYPTION POLICY 20

1.0 Purpose 20
2.0 Scope 20
3.0 Policy 20
4.0 Enforcement 20
5.0 Definitions 20
6.0 Revision History 20

PERSONNEL POLICY RELATED TO INFORMATION SECURITY 21

GRANTD EQUITIES ETHICS POLICY 22

OVERVIEW 22
PURPOSE 22
SCOPE 22
POLICY 22
Executive Commitment to Ethics 22
Employee Commitment to Ethics 22
Company Awareness 23
Maintaining Ethical Practices 23
Unethical Behavior 23
Enforcement 23

IT SECURITY POLICIES AND PROCEDURES - RISK ASSESSMENT POLICY 24

1.0 PURPOSE 24
2.0 SCOPE 24
3.0 ACCOUNTABILITY 24
4.0 RISK ASSESSMENT PROCESS 24
5.0 REMEDIATION 24
6.0 ENFORCEMENT 24
7.0 DEFINITIONS 24
7.0 REVISION HISTORY 25

APPENDIX A: AUDIT CHECKLIST 27

APPENDIX B: RECORDS RETENTION SCHEDULE, STORAGE & ASSETS 31

STOCKOPTER RECORD RETENTION SCHEDULE 31
RECORD STORAGE INFORMATION 31
STOCKOPTER ASSET INVENTORY 32
HARDWARE ASSET CLASSIFICATION AND HANDLING 32

APPENDIX C: STOCKOPTER.COM APPLICATION NETWORK DIAGRAM 33

APPENDIX D: PATCH MANAGEMENT POLICY 34

Data Security Policy

In General

Access to computer resources (computers, network directories and files, etc.) is restricted on a "need-to-know" basis. Management is the sole arbiter of this need.

This document is broken down into several broad categories. All GRANTD employees are required on an annual basis to document that they have reviewed and will abide by the terms, policies and procedures set forth herein.

The goal is to achieve and sustain a reasonable level of data security and privacy consistent with the specific needs of our customers. As we acquire new customers, and as the needs of existing customers change, these policies and procedures will be modified accordingly.

These policies and procedures are reviewed annually and approved by senior management.

Information Security Organization

Organizational responsibilities are as follows:

- The CEO shall have ultimate responsibility for corporate information security and for delegation of information security responsibilities.
- The CTO shall have responsibility for overall management of the company's data security policies and procedures.
- Each employee and contractor who may be exposed to confidential information shall be responsible for protecting said information according to this policy.

Data Security

- Handling – Policies and procedures for handling customer confidential information:
    - All customer confidential information that is electronically provided to GRANTD is immediately placed in a secure (limited access) folder on the GRANTD file server, which is hosted by Dropbox. Access to secure directories on the GRANTD file server is limited at all times to management and professional staff.
    - Customer client data entered or imported into StockOpter.com is stored in a secure SQL database. Personally identifiable information (i.e. Participant Name, ID, and Email Address) are encrypted using a 128 bit key. The database activity log is reviewed quarterly to insure against unauthorized access.
    - The data that is used to create reports during which time, only GRANTD personnel or third party service providers authorized by GRANTD are provided with access to this data. This may include database administrators, professional staff and technology resources.
    - If customer client deliverables are generated by GRANTD staff, these are placed in the secured directory on the GRANTD file server.

    - Where data is received at external "hosting" site, data security provisions at that site must meet GRANTD and client company security requirements.

- Physical data security – Measures taken to secure hardware containing personally identifiable information at GRANTD premises.

    - All confidential customer data is secured on either the GRANTD application server (StockOpter) or in a secure directory on the GRANTD file server (Dropbox).

    - Where data is received at external "hosting" site, data security provisions at that site must meet GRANTD and client company security requirements

Software Development

- All application development will utilize the Software Development Life Cycle (SDLC) methodology to create high-quality and secure SaaS software via the following phases:
    - Requirements Analysis
    - Planning
    - Architectural Design
    - Software Development
    - Testing
    - Deployment

Access Management, Entitlement and Password Policies

1) All account passwords expire every three months requiring each user to re-assert a new password and users may not reuse the previous 8 passwords

2) Passwords must be at least 8 characters long and contain one capitalized letter, one our more numeric values and a special character

3) GRANTD servers do not use the default "Administrator" account. In its place, particular accounts are assigned to the 'Administrator' group

4) Sharing of user account or password with any person is prohibited

5) Accounts for consultants or temporary employees are disabled or deleted within 24 hours of termination of agreement

6) Review of access privileges and user account is done quarterly by management

7) System access to either internally or externally hosted systems is limited to the information and functionality that is required by the employee to do their job. Access to internal systems is granted to authorized employees by creating a user profile on the server and providing them with a temporary password. Access to external systems (i.e. StockOpter.com) is done by providing the employee with a user ID and temporary password.

8) Upon termination, the employee's user access of all internal and external systems is removed immediately by eliminating their profile and user IDs and by changing their passwords

Backups

1) Backups are run daily and retained for 5 days by our third-party hosting site, Microsoft Azure.

2) File restoration procedures are tested annually.

3) Remediation of data corruption, Restoration and Integrity testing are also tested annually.

Disaster recovery

1) The GRANTD main business location is:
    a) 2440 Junction Place, Suite 300, Boulder, CO 80301
    b) Or, other location to be determined by management

2) Computers will be replaced from Dell, Inc.
    a. Dell Computers - (987) 654-4321
    b. Or, other vendor as determined by management

3) The network administrator will be responsible for restoring the server and its contents

Security Incident Policy

1) Any potential or suspected breach of computer security or incidents affecting availability is required to be reported immediately to the CEO by employees or by the hosting service providers.

2) At the CEO's request, qualified persons will be charged with investigating and reporting upon the cause of the breach, potential breach or availability incident, identifying the impacted parties and suggesting a corrective course of action. Within 24 hours of discovery of a security breach, the CEO or designees will notify customers whose data might have been compromised of the details of the incident and the efforts underway to resolve the situation.

3) Security breaches, suspected breaches and incidents affecting availability will be investigated within 3 hours of the incident and resolved or escalated within 12 hours.

4) If the incident can't be resolved within 12 hours of identification the CEO will escalate the incident and additional qualified persons will be charged to provide a corrective course of action. Escalated incidents will be reviewed every 12 hours by the CEO until they are resolved. Affected customers will be notified within 24 hours of the escalation and appraised of the status of the situation every 24 hours until and upon resolution.

Outside contractors

1) Outside contractors given access to GRANTD data or computer resources are required to sign a Privileged Authority Agreement prior to any work. In this document, they will explicitly agree to be held to local, state and federal laws concerning data privacy and security.

Network security

1) All passwords to network devices, including routers, firewalls, cable modems etc. are changed from factory defaults, when possible

2) A written list of all network devices, including Administrator accounts on the network, are provided to the CEO and updated quarterly.

3) Access logs are reviewed quarterly by the network administrator

Change Control / Change Management

1) System patches are applied according to the GRANTD Patch Management Policy (Appendix D)

2) All in-house applications have separate development, test/QA and production environments

3) All modifications, patches or content changes are coordinated by the CTO

4) Changes are specified in writing and are promoted to the test/QA environment when ready

5) All modifications are thoroughly tested prior to promotion to the production environment

6) A final test of the modification is done on the production system

Data Transfer and Decommissioning

1) All data transfers involving customer confidential data is done via a secured connection or methodology

2) Customer confidential data will be decommissioned upon written request and expunged from application servers.

Physical Site Security

1) GRANTD business offices physical security measures:
   a. File/application servers are NOT hosted onsite
   b. Access control procedures
   c. Emergency procedures
   d. A clear desk policy
   e. Secure file cabinets and document shredding bin
   f. Building closed circuit TV surveillance
   g. Non-employee escort policy

2) Offsite application and file server physical security measures:
   a. Single point entry with guards
   b. 24 hours facility surveillance
   c. Electronic card access control for interior areas
   d. Enhanced access control measures for server rooms including biometrics, keys, and man-traps
   e. All physical access is permitted to authorized employees and customers ONLY

Security Awareness Program

1) The importance of data security is regularly communicated by management through verbal and written communications.

2) Annually each employee and contractor will acknowledge by signature that they have reviewed the Grantd Equities policies related to data privacy and security and will comply with them.

Asset classification and handling

1) Information assets are classified as follows:

    a. Computer assets including:
        i. All PCs and laptops
        ii. All servers
        iii. All hard disks which have ever been in a PC
        iv. Removable media

    b. Software assets include
        i. Operating systems
        ii. Third party application software
        iii. Grantd Equities program and ASP products

2) A list of all assets is maintained and reviewed annually

3) For assets outside GRANTD premises, the inventory includes
    a. The name of the person in possession of the equipment
    b. The reason for the possession
    c. The anticipated date of return to GRANTD
    d. Mobile computing devices shall at all times be attended or in a physically secured location such as the Grantd Equities offices or a locked home environment. When traveling mobile computing devices left in a hotel room must be physically locked in a safe or secured to an immovable object.

4) Unused equipment
    a. Hard disks are removed and physically destroyed prior to disposal
    b. Unneeded data storage devices (hard disks) are cleaned and disposed of

5) All removable media such as back-up files, laptops, flash drives, etc. will be encrypted such as to protect their content in the event of theft or loss.

PC and Server Security

1) All GRANTD PCs, internal servers and 3rd party hosted servers are required to have anti-virus software installed and running.

2) Anti-virus updates for all PCs and servers are pushed on a daily basis and as required. GRANTD PCs and internal servers are also scanned for viruses randomly by an IT consultant. Hosted servers are scanned for viruses nightly.

3) Third party confidential or customer information will not be stored on any mobile devices.

Other Policies

1) Use of GRANTD systems to attack other computer systems, internal or external to GRANTD, is a violation of this policy subject to administrative, civil, and/or criminal sanctions.

2) Attempting to circumvent security or administrative access controls for computer resources is a violation of this policy, as is assisting someone else or requesting someone else to circumvent security or administrative access controls.

3) Users are responsible for managing their passwords and for all actions and functions performed by anyone logging on with their User Id's.

4) Violations of this Computer Security Policy will be reported to the GRANTD Vice President of Administration or to the CEO.

5) Persons violating any portion of this Computer Security Policy may be subject to internal GRANTD disciplinary action, up to and including dismissal, as well as other administrative, civil, and/or criminal sanctions.

Enforcement

All employees/contractors are required to review and sign this document and new employees are provided with mandatory training to insure compliance. Signatures are tracked and reported to Senior Management.

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

Employee/Contractor Acknowledgement:

I hereby acknowledge that I have read and understand Grantd Equities Data Security and Privacy Policy Handbook and agree to abide by all terms and conditions set forth herein.

_____ _____

Signature Printed Name

_____

Date

Employer Acknowledgement:

_____ _____

Signature Printed Name

_____ _____

Date Title

Appendix A – Security Access Warning Message

Successful prosecution of unauthorized access to GRANTD computerized systems requires that users are notified prior to their entry into the systems that the data is owned by GRANTD and that activities on the system are subject to monitoring. All employees and contractors will be required to sign an acknowledgement of the following message upon employment:

> The computer systems at GRANTD are to be used only by authorized individuals, and all others will be prosecuted. Activities on these systems may be automatically logged and are subject to review. All data on these systems is the property of Grantd Equities, Inc., which reserves the right to intercept, record, read or disclose it at the sole discretion of authorized individuals. System administrators may disclose any information on or about this system to law enforcement or other appropriate individuals. Users should not expect privacy from system review for any data, whether business or personal, even if encrypted or password-protected. GRANTD takes precautions to prevent the disclosure of confidential information. Use of these systems constitutes consent to these terms.

Employee Initials

IT Security Policies and Procedures - Information Sensitivity Policy

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 Grantd Equities, Inc. (GRANTD) 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 you can take to protect Grantd Equities, Inc. Confidential information. 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 your manager. Questions about these guidelines should be addressed to Info sec.

Scope

All Grantd Equities, Inc. information is categorized into four main classifications:

- GRANTD Public Information
- GRANTD Administrative Information
- GRANTD Confidential Information
- Third Party Confidential Information

GRANTD 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 Grantd Equities, Inc.

GRANTD Administrative Information presents little or no risk if disclosed and does not require any special handling.

GRANTD Confidential Information 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. This information shall be designated as GRANTD Confidential Restricted and shall be protected at the highest level and will generally not be shared with third parties. Also included in GRANTD 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. This information will be designated GRANTD Confidential and may be selectively shared with third parties.

Third Party Confidential Information is confidential information belonging or pertaining to another corporation which has been entrusted to Grantd Equities, Inc. 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 needs to be marked by the third party as "Confidential" to be treated as such. Also included in this category is third party customer information that is stored on StockOpter.com.

Refer to the "Protection Level" table below for details on each security class.

Grantd Equities, Inc. personnel are encouraged to use common sense judgment in securing Grantd Equities, Inc. 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

Protection Level by Security Class

Security Class	Marking (if required)	Access Outside of GRANTD	Storage
GRANTD Public Information	None	Yes	Open
GRANTD Administrative Information	None	Under limited circumstances	Open
GRANTD Confidential Information	Yes	Limited at management discretion	Locked file cabinet (standard file cabinet locks)
GRANTD Confidential Restricted Information	Yes	None	Locked file cabinet (High security file cabinet lock)
Third Party Confidential Information	Yes by third party	None	Locked file cabinet (High security file cabinet locks)
Third Party Confidential: Customer Information on StockOpter.com	None	Third Party	Dedicated and secured server on Microsoft Azure. Personally identifiable information is encrypted.

Enforcement

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

Terms & Definitions

Appropriate measures
To minimize risk from an outside business connection. Grantd Equities, Inc. computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Grantd Equities, Inc. corporate information, the amount of information at risk is minimized.

Configuration of Grantd Equities, Inc.-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
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Grantd Equities, Inc. is done via a license. Please contact the appropriate support organization if you require a license.

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 or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac'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.

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 Grantd Equities, Inc.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key 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 take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that Grantd Equities, Inc. has control over its entire distance. For example, all Grantd Equities, Inc. networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link.

Revision History

- June 2020

- June 2021
- May 2022
- May 2023
- July 2024

IT Security Policies and Procedures - Acceptable Use Policy

1.0 Overview

Grantd Equities, Inc.’s intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Grantd Equities, Inc.’s established culture of openness, trust and integrity. Grantd Equities, Inc. is committed to protecting Grantd Equities, Inc.'s 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 Grantd Equities, Inc. 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 Grantd Equities, Inc. 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.

2.0 Purpose

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

3.0 Scope

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

4.0 Policy

4.1 General Use and Ownership

1. While Grantd Equities, Inc.'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Grantd Equities, Inc. Because of the need to protect Grantd Equities, Inc.'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to Grantd Equities, Inc.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. If there is any uncertainty, employees should consult their supervisor or manager.

3. Grantd Equities, Inc. recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see Grantd Equities, Inc.'s Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Grantd Equities, Inc.'s Acceptable Encryption Policy.
4. For security and network maintenance purposes, authorized individuals within Grantd Equities, Inc. may monitor equipment, systems and network traffic at any time, per Grantd Equities, Inc.'s Audit Policy.

5. Grantd Equities, Inc. reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for 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 confidential, 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. System level passwords should be changed every six months; user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

4. Use encryption of information in compliance with Grantd Equities, Inc.'s Acceptable Encryption Use policy.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Grantd Equities Data Privacy and Security Policy".

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

7. All hosts used by the employee that are connected to the Grantd Equities, Inc. Internet/Intranet/Extranet, whether owned by the employee or Grantd Equities, Inc., shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

8. Employees must not open e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

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 Grantd Equities, Inc. authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Grantd Equities, Inc.-owned resources.

The lists below are by no means exhaustive but attempts to provide a framework for activities which fall into the category of unacceptable use.

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 Grantd Equities, Inc.

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 Grantd Equities, Inc. 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, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a Grantd Equities, Inc. 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 Grantd Equities, Inc. 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 Grantd Equities, Inc. 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 terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Grantd Equities, Inc. employees to parties outside Grantd Equities, Inc.

4.4. 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 Grantd Equities, Inc.'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Grantd Equities, Inc. or connected via Grantd Equities, Inc.'s network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

8. Any outgoing email that contains customer proprietary or personally identifiable information shall be encrypted in accordance with the GRANTD encryption policy.

4.5. Blogging

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

2. Grantd Equities, Inc.’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any New Worth Strategies, Inc. confidential or proprietary information, trade secrets or any other material covered by New Worth Strategies, Inc Confidential Information policy when engaged in blogging.

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

4. Employees may also not attribute personal statements, opinions or beliefs to Grantd Equities, Inc. when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Grantd Equities, Inc.. Employees assume any and all risk associated with blogging.

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

5.0 Enforcement

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

6.0 Definitions

Term	**Definition**
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Acceptable Encryption Policy

1.0 Purpose

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. 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.

2.0 Scope

This policy applies to all Grantd Equities, Inc. employees and affiliates.

3.0 Policy

All customer confidential or client private data residing on GRANTD servers or outside hosted sites will be encrypted. A list of all such encrypted fields, tables, or files will be maintained for audit purposes.

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate'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. Grantd Equities, Inc.'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 approved by the customer whose data is to be protected. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement

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

5.0 Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data.
Asymmetric Cryptosystem	A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

6.0 Revision History

Personnel Policy Related to Information Security

In order to minimize the risk that Grantd Equities employees and contractors would violate company information security policies whether deliberately or inadvertently, the company has implemented the following practices:

1. Recruiting and selection of employees
    a. Drug testing
    b. Criminal background check
    c. Credit check
    d. Personal references check
    e. Interview process (multiple interviews)

2. Engagement of independent contractors and consultants
    a. Drug testing
    b. Criminal background check
    c. Credit check
    d. Personal references check
    e. Interview process (multiple interviews)

3. Employee training on information security
    a. Annual review of Data Policy Security Handbook
    b. Periodic reviews at team meetings

4. Annual review and sign-off by employees and contractors on the company's information security policies

5. Periodic audit of each employee and contractor for compliance with company information security policies.

6. Employee or Contractor termination. The following actions shall be taken:
    a. At time of termination employee is escorted from the premises.
    b. Keys if any are collected.
    c. Computer profiles and passwords are invalidated.
    d. Review of all files on employee/contractor systems. Expunged as appropriate.

Grantd Equities Ethics Policy

Overview

The Grantd Equities, Inc. ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Grantd Equities, Inc. employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

Grantd Equities, Inc. is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Grantd Equities, Inc. addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

Grantd Equities, Inc. will not tolerate any wrongdoing or impropriety at anytime. Grantd Equities, Inc. will take the appropriate measures and act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

Purpose

Our purpose for authoring a publication on ethics is to emphasize the employee's and consumer's expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Grantd Equities, Inc., including all personnel affiliated with third parties.

Policy

Executive Commitment to Ethics

i. Top management within Grantd Equities, Inc. must set a prime example. In any business practice, honesty and integrity must be top priority for executives.

ii. Executives must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert executives to concerns within the work force.

iii. Executives must disclose any conflict of interests regard their position within Grantd Equities, Inc.

Employee Commitment to Ethics

i. Grantd Equities, Inc. employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

ii. Every employee needs to apply effort and intelligence in maintaining ethics value.

iii. Employees must disclose any conflict of interests regarding their position within Grantd Equities, Inc.

iv. Employees will help Grantd Equities, Inc. to increase customer and vendor satisfaction by providing quality product s and timely response to inquiries.

Company Awareness

i. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

ii. Grantd Equities, Inc. will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

Maintaining Ethical Practices

i. Grantd Equities, Inc. will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs to consistently maintain an ethical stance and support ethical behavior.

ii. Employees at Grantd Equities, Inc. should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

iii. Annually all employees will review and sign-off on this Ethical Practices Policy. At this time, any concerns regarding the code can be addressed.

Unethical Behavior

i. Grantd Equities, Inc. will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

ii. Grantd Equities, Inc. will not tolerate harassment or discrimination.

iii. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

iv. Grantd Equities, Inc. will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

v. Grantd Equities, Inc. employees will not use corporate assets or business relationships for personal use or gain.

vi. Money laundering, bribery or corruption of any kind is unacceptable behaviour.

Enforcement

i. Any infractions of this code of ethics will not be tolerated and Grantd Equities, Inc. will act quickly in correcting the issue if the ethical code is broken.

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

IT Security Policies and Procedures - Risk Assessment Policy

1.0 Purpose

To empower the selected audit firm, consultant or GRANTD employee to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope

Risk assessments can be conducted on any entity within Grantd Equities, Inc. or any outside entity that has signed a *Third Party Agreement* with Grantd Equities, Inc.. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained. These assessments may be conducted by a selected audit firm, by Grantd Equities management, or through required submission of outside entity's own audited results or response to GRANTD written assessment questions.

3.0 Accountability

The execution, development and implementation of remediation programs are the joint responsibility of the selected audit firm and the management responsible for the systems or functions being assessed. Employees are expected to cooperate fully with any risk assessment being conducted on systems for which they are held accountable.

4.0 Risk Assessment Process

The process consists of an annual audit of all key provisions of the company's information security policies. This may be accomplished by one or more of the following methodologies:

- Team reviews
- Review of outside entity's own audited results or response to GRANTD written assessment questions.
- Interviews with individual employees and contractors
- Physical reviews
- Tests of system capabilities

See Appendix A for current Audit Check List

5.0 Remediation

Any vulnerability items discovered through a periodic risk assessment (RA) will be given a severity classification based on the combination of the likelihood of exploitation and the severity of exploitation. Rating classes of Critical, High, Medium, and Informational may be assigned to vulnerabilities. All classes must be remediated immediately with the exception of informational, which does not require remediation. Remediation programs must be approved by the CTO and follow standard quality assurance processes.

6.0 Enforcement

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

7.0 Definitions

Terms	**Definitions**
Entity	Any business unit, department, group, or third party, internal or external to Grantd Equities, Inc., responsible for maintaining Grantd Equities, Inc. assets.

Risk	Those factors that could affect confidentiality, availability, and integrity of Grantd Equities, Inc.'s key information assets and systems. the selected audit firm is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History

- April 2026

Appendix A: Audit Checklist

Audit Question	Practice	Audit Procedure	Category	Audit Period	Policy	Responsible Party
Which physical and logical assets does the supplier maintain an inventory of? (For example, hardware, software, databases, applications)	Hardware, software (including OS, utilities, and applications). Physical inventory review annually in conjunction with county property tax submission.	Audit list against assets. Update as required	Asset acceptable use	Annual	Asset Classification & Handling	CTO
Within the organization, who typically owns information assets? How often do these owners review and approve access to their information assets?	Work stations: CTO for common workstations used for testing, each employee for the workstations they use, CTO for server and related hardware (router, firewall, hubs, etc.). Annual sign off on security of assets by owners.	1. Review all workstations to ensure that only valid users have access. 2. Inspect all workstation hard drives to ensure that there is no customer confidential data is absent or protected. 3) sign off by owner of each asset that policies are being followed	Asset acceptable use	Quarterly	Data Security	CTO,
Describe the information classification levels used to classify information in terms of value, legal requirements, sensitivity, and/or criticality. .	GRANTD Confidential Restricted, GRANTD Confidential, GRANTD Administrative, GRANTD Public	Audit each information owner for compliance with classification levels.	Asset acceptable use	Rolling Annual	Information Sensitivity	CTO
Does your company have a documented records retention and destruction schedule for StockOpter? Please describe.	A schedule showing the length of time for which each class of document or record is to be retained or destroyed	Interview each information owner for compliance with retention schedule	Asset acceptable use	Annual	Handbook	CTO
Do you have a formal risk assessment process? Please provide an overview.	Annual risk assessment audit to be conducted by CTO in accordance with the Risk Assessment Policy and Checklist. Results of audit will be reviewed with CEO and Board	Review and resolve potential risks and impacts against risk list	Audit	Annual		CTO
How often do you perform formal business impact analyses, and when was the last one performed?	In the past, business impact analysis has been conducted informally. Going forward it will be performed formally on an annual basis	As part of risk assessment evaluate potential impacts and appropriate resolution within Business Contingency Policy	Audit	Annual	Risk Assessment	CTO
Data Security Policy	Account lists (Network users), names, and directory access are reviewed quarterly by management	Review to ensure policy is being followed	Data Security	Quarterly	Network Account Security & User Access	Security Specialist
Data Security Policy	File restoration procedures are tested	Sign off by IT consultant that restoration procedure has been tested	Data Security	Annual	Network Account Security & User Access	Security Specialist
Data Security Policy	Access logs are reviewed regularly by the network administrator.	Sign off by IT consultant that access logs have been reviewed	Data Security	Monthly	Network Account Security	Security Specialist

How does the company ensure that client data stored in StockOpter.com is secure?	All personally identifiable information (client name, ID and email) are encrypted using a 128 bit key.	The database activity log is reviewed quarterly to insure against unauthorized use.	Data Security	Quarterly	Data Security	Security Specialist
Data Sensitivity Policy	In -house: data files are uploaded or downloaded from server over internal network.	Employee PCs audited for sensitive data.	Data Security	Annual	Data Transfer	CTO
Data Sensitivity Policy	Out -house: All data is transferred via secure method as specified by the vendor/customer/consultant.	Annual sign off by IT consultant	Data Security	Annual	Data Transfer	Security Specialist
Data Sensitivity Policy	All GRANTD PCs will have anti-virus software installed and running. Virus files automatically updated daily. Scans automatically triggered weekly.	Random audits of workstations at least once per month	Data Security	Quarterly	PC Security	CTO
Data Sensitivity Policy	To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.	Representation by CTO	Data Security	Annual	Information Sensitivity	CTO
Data Security Policy	System level and User level passwords should be changed every six months. Passwords must be at least 6 characters long and contain one capitalized letter and one or more numeric values.	CTO to get sign off from IT consultant that procedures are compliant	Data Security	Quarterly	Acceptable use	Security Specialist
Data Security Policy	All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 30 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.	Periodic inspection by CTO or delegate. Representation by each owner	Data Security	Quarterly	Acceptable use	CTO
Data Security Policy	All hosts used by the employee that are connected to the Grantd Equities, Inc. Internet/Intranet/Extranet, whether owned by the employee or Grantd Equities, Inc., shall be continually executing approved virus-scanning software with a current virus protection program.	Quarterly audit by IT Consultant for virus protection and data transfer security	Data Security	Quarterly	PC Security	Security Specialist
Describe the procedures in place in the case of a privacy incident?	Immediate notification to CEO for appropriate and timely resolution. Customers who might be impacted will be notified within 24 hours as specified in the GRANTD Data Security Policy	Policy sign off by all employees and contractors	Incident management	Annual	Security Incident	CTO
Does the supplier perform risk assessments on its employees & third parties? If yes, what do these risk assessments cover?	Criminal, drug, and credit checks at the time of engagement of individual/independent contractors and consultants. Where possible,	Check records of any new hires/engagements for compliance	Personnel security	Annual	Personnel	CTO

	character references are checked with people known to GRANTD.					
What actions do managers take to ensure employees understand the consequences of breaking company policies?	Incorporated in company policies reviewed and signed by employees annually	Check records for current signed policy statements	Personnel security	Annual	Personnel	CTO
How often do employees receive security awareness training?	Each security/risk topic discussed at least annually in team meetings.	Review data/security training check list to ensure that training has been conducted or scheduled for a team meeting before the anniversary of the last audit	Personnel security	Annual	Security Awareness	CTO
How does GRANTD handle the termination of employees?	At time of termination employee is escorted from the premises. Keys if any are collected, Computer profiles and passwords are invalidated within 24 hours and security system password is invalidated. See termination check list.	Review records to ensure that termination practices have been invoked for all employees/contractors terminated since last audit	Personnel security	Quarterly	Personnel	CTO
How does GRANTD handle the termination of consultants/temporary employees?	Accounts for consultants or temporary employees are disabled or deleted within 24 hours of termination.	GRANTD has a termination checklist that is used to sign off on all tasks necessary at time of termination. CTO is responsible for making sure all tasks are completed.	Data Security	Quarterly	Network Account Security & User Access	CTO
How often do you require your employees to sign non-disclosure agreements or confidentiality agreements?	Annually	Check records for current signed NDA, IP, and Confidentiality agreements	Personnel security	Annual		CTO
Data Security Policy	Outside contractors given access to GRANTD data or computer resources are required to sign a “Privileged Authority” document prior to any work. In this document, they will explicitly agree to be held to local, state and federal laws concerning data privacy	Review Independent Consultant agreements at time of hire and annually thereafter	Personnel security	Annual	Outside Contractors	CTO
Data Security Policy	Contractors with data access are also subject to the provisions of our Risk Assessment Policy.	Review records to ensure compliance	Risk Assessment	Annual	Risk Assessment	CTO
If third-parties are used, describe how these third-party service providers are monitored for compliance with security standards and contract agreements.	Provide/update answers to questions contained herein relevant to the service provided to company. These answers will be reviewed by GRANTD annually and made available to company.	Check for current sign off on previous or modified security/privacy questionnaire	Third party monitoring	Annual	Outside Contractors	CTO
How does GRANTD check for unauthorized access or copying of participant confidential data in the	GRANTD management reviews database and application activity logs	Create activity log and review for unauthorized access of participant data.	Personnel security	Quarterly	Personnel	Security Specialist

StockOpter.com database by development personnel?	for versions of StockOpter.com hosted by Microsoft Azure.					
What is the process to assess security risks to determine areas of vulnerability?	An annual audit of all key provisions of the company's security policy is reviewed.	The review is done annually via a team meeting.	Security Risk	Annual	Risk Assessment	Team
Business Continuity Plan	Updates will be made in response to changes in the business environment	Annual review of the Plan to verify information is current	Biz Continuity Plan	Annual		CTO

Appendix B: Records Retention Schedule, Storage & Assets

StockOpter Record Retention Schedule

Customer Client Records	Indefinitely or upon customer request or account termination
Customer Correspondence (general)	2 yrs.
Correspondence (legal & important matters only)	Permanently
Internal audit and miscellaneous reports	3 yrs
Customer Invoices	3 yrs
Sales records	7 Yrs
Trademark registrations & copyrights	Permanently
StockOpter support and training information	Permanently

Record Storage Information

Source	Location	Type	Classification	Confidentiality level
Customer Operational Records	Fileserver	Docs/Application	Operations Support	GRANTD Confidential
Customer Contracts	Fileserver	Files/Documents	Operations Support	GRANTD Admin
Industry Information	Fileserver/Cabinet	Publications	Marketing Support	GRANTD Public
Customer / Prospect Marketing Information	Fileserver	Documents	Marketing Support	GRANTD Public
Notes from Clients' Discussions	Fileserver	Files/Documents	Operations Support	GRANTD Confidential
Former clients archive	Fileserver	Files/Documents	Corporate Records	GRANTD Confidential

StockOpter Asset Inventory

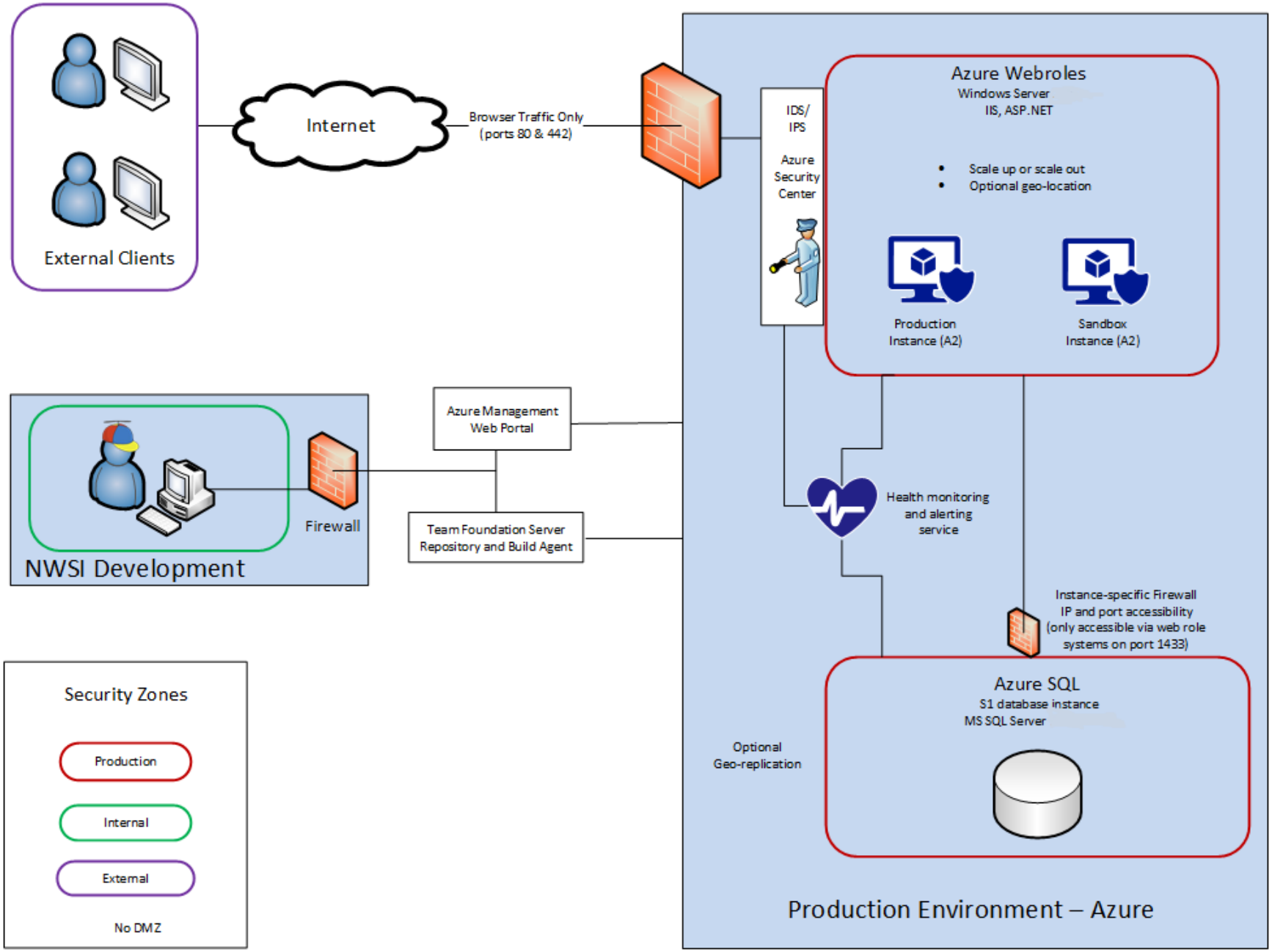
OFFICE ASSETS	COMPUTER HARDWARE ASSETS
Office Furniture	Laptops (2)
File Cabinets	Additional monitors (3)
	22" LCD monitor
Office Machines	24" LCD Monitor
Epson 4750 Copier/Fax/Scanner	
Binding Machine	
Phone system	

SOFTWARE INVENTORY
MS OS Software
Windows Server 2022 (Azure)
SQL Server
Windows 10 (2 copies factory installed – B. Dillhoefer, K. Pape machines)
MS Office Software
Microsoft 365
Misc. Software
Aspose'.word.net - Web based document generation for StockOpter
DevExpress
Carbonite
Webroot Secure Anywhere 9.0
Sectigo

Hardware Asset Classification and Handling

Information Source	Location	Classification	Type of Information
Dillhoefer Computer	Office	Function: Sensitive Availability: High Integrity: High	Database administration Operations Support Customer and Product Admin

Appendix C: StockOpter.com Application Network Diagram



Appendix D: Patch Management Policy

Purpose
This policy ensures that all systems supporting the Company's SaaS application on Microsoft Azure remain secure, stable, and up to date through timely application of operating system, platform, and application patches.

Scope
Applies to all Azure-hosted infrastructure, including virtual machines, containers, PaaS services, databases, networking components, CI/CD pipelines, and third-party software dependencies. Covers all employees and contractors responsible for system maintenance.

Responsibilities
- **Engineering/DevOps:** Maintain patch automation via Azure Update Manager, validate patches in staging, deploy to production, and monitor patch success.
- **Security:** Track vulnerabilities, validate compliance, and review patch exceptions.
- **Management:** Approve maintenance windows and ensure adequate resources for patching.

Patch Classification & Timelines

Severity Levels		Remediation Target
Critical	Zero-days, active exploits	24–72 hours
High	Major vulnerabilities, privilege escalation	7 days
Medium	Stability fixes, non-exploited issues	30 days
Low	Minor updates	90 days

Azure Defender for Cloud and CVSS scores guide severity classification.

Patch Management Process
1. **Discovery:** Azure Update Manager identifies missing OS patches
2. **Testing:** Patches are applied to staging environments and validated through automated and manual tests.
3. **Deployment:** Production patching occurs during approved maintenance windows using automated orchestration.
4. **Verification:** Azure Monitor and Log Analytics confirm patch success and system stability; failed patches are remediated or rolled back.

Logging & Monitoring
- Patch events and system logs are collected in Azure Monitor and Log Analytics.
- Alerts notify teams of patch failures, anomalies, or unpatched critical vulnerabilities.
- Defender for Cloud provides continuous vulnerability assessment.

Protection of Logs
- Logs are stored with immutable retention settings.

- Access is controlled via Azure AD and RBAC.
- Activity Logs are inherently tamper-proof.
- Data is replicated across availability zones for durability.

Exceptions
If a patch cannot be applied, a documented exception must be submitted with compensating controls. Exceptions are reviewed every 90 days.

Compliance
Supports SOC 2, ISO 27001, NIST 800-53, and customer security requirements.

Review Cycle
This policy is reviewed annually or after significant infrastructure changes.