# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| Section<br>Question | Responses | Requested Attachments | Attachments |
|---|---|---|---|
| ********** **Business Information** ********** | | | |
| **A - Respondent Contact Information** | | | |
| Name: | Bill Dillhoefer | | |
| Job Title: | President, CEO | | |
| Email: | bdillhoefer@networthstrategies.com | | |
| Phone: | 541-383-3899 x102 | | |
| **B - Company Profile** | | | |
| What is the name of your organization? | Net Worth Strategies, Inc. | | |
| Please provide URL address of your organization webpage? | https://networthstrategies.com/ | | |
| How long has your organization been in business? | 24 year | | |
| What is the overall number of employees in your organization? | 4 | | |
| Please provide a list of all countries in which your organization operates | USA only | | |
| Please indicate any regulator which supervises or examines your organization | None. We are a software company. | | |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | |
|---|---|
| Has your organization experience any major security incidents? | No |
| **C - Service Profile** | |
| Please provide name(s) and description(s) of all service(s) which are planned to be or are already provided to customers | StockOpter.com: application for performing equity compensation tracking, risk analysis, and tax and cash flow strategy modeling |
| What is the nature of the services/transactions involved? | Enable financial advisory firms to provide equity compensation recipient with guidance. |
| If possible, please provide a URL address where these services are described | https://stockopter.com/ |
| How many employees are involved in providing the service to customers? | 4 |
| How many employees have access to customer data? | 2 |
| From which countries will the service provided to customers be operated? | USA |
| Is this a shared or dedicated service? | Shared Service |
| Is the service in question based on cloud technology such as SaaS, PaaS or IaaS? | Yes |
| Are any aspects of the service outsourced? | Yes |
| Please describe what is outsourced, the name of the contracted party and the country of operation. | The StockOpter.com application is currently hosted on a Microsoft Azure cloud server in Des Moines, IA. |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | | |
|---|---|---|
| Please provide details of the data/information that will be used/accessed by your organization to provide the service | Equity compensation grant information and related financial assumptions. | |
| Does your company receive Personal Identifiable Information (PII)? | NO, client first and last names and email addresses are optional. | |
| Is all the data received from customers masked/anonymized? | N/A | |
| Describe how your organization will receive the data needed to provide the service. | Users manually type the information into StockOpter.com | |
| Does your organization have a technical or business Data Flow Diagram associated with the service? | Yes | Network Diagram - Azure.pdf |
| What is the expected volume of data required to perform the service? | Low | |
| How often is data exchanged? | Users add and update data periodically. | |
| Will your organization need access to customer systems/applications to perform the service? | No | |
| **D - Address Details** | | |
| Main office address: | 62910 O.B. Riley Rd.<br>Suite 300<br>Bend, OR 97703<br>Mailing address: PO BOX 8364, Bend, OR 97708 | |
| Backup office address: | 1449 NW Saginaw Avenue, Bend, OR 97703 | |
| Primary Data Center address: | Microsoft Azure | |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | | |
|---|---|---|
| | 8855 Grand Ave<br>West Des Moines, IA 50266 | |
| Backup Data Centers address: | Alternate Azure facilities | |
| Are there any additional location(s) where customer information is stored, processed, archived, viewed or destroyed? | No | |
| | | |
| ********** **Organizational Level Controls** ********** | | |
| | | |
| **1 - Risk Management** | | |
| Does your organization have a formal (documented, approved, published, communicated, and implemented) Risk Management program/framework? | Yes | NWSI Data Security and Privacy Policies Handbook.pdf |
| Which function is assigned to maintain and review the program/framework? | Vice President of Administration | |
| Does your organization regularly perform information risk assessments for critical processes, applications and/or infrastructure? | Yes | |
| Which function is responsible for completion of the assessments? | Vice President of Administration | |
| How often are risk assessments performed? | As required by customers but at least annually. | |

| | | |
|---|---|---|
| How does your organization prioritize / classify risks identified in the assessment process? | High: Urgent/critical, address immediately<br>Medium: Important but not urgent, address ASAP<br>Low: Low risk, address after other risks | |
| Does your organization formally document information risk analysis' outcomes? | No | |
| Is the risk assessment process supported by the existence of a risk inventory? | No | |
| | | |
| **2 - Vendor Risk Management** | | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Vendor Risk Management program/framework? | Yes | NWSI Data Security and Privacy Policies Handbook.pdf |
| Do all vendors that deliver sub-contracted services to your organization have to complete this program? | Yes | |
| Does this program include a review of the financial position of an external vendor? | Yes | |
| Is a vendor risk assessment process part of this program? | Yes | |
| What is in the scope of the assessment of an external vendor? | Background check and references. | |
| Does the vendor risk assessment process need to be completed before authorization is given to contract with an external vendor? | Yes | |

| | | |
|---|---|---|
| How is this control enforced? | By VP of Administration | |
| Contracts with external vendors cover the following considerations: | Information security<br>Data protection<br>A right to carry out a review or assessment for regulatory, audit or compliance purposes | |
| Does your organization undertake periodic re-assessment of approved external vendors? | Yes | |
| What is in the scope of the periodic re-assessment of approved external vendors? | Review audit information | |
| How often are periodic re-assessments performed? | Annually | |
| Does your organization have any external connections to third parties? | No | |
| | | |
| **3 -Security Policy** | | |
| Does your organization have formal (documented, approved, published, communicated and implemented) information security policies and procedures? | Yes | NWSI Data Security and Privacy Policies Handbook.pdf |
| Please list all information security policies and procedures. | In the handbook | |
| How is it ensured that policies and procedures are periodically reviewed and verified to reflect organizational and technological changes? | They are reviewed and updated continually based on customer feedback and surveys. | |

| | |
|---|---|
| Which function is responsible for keeping policies' content up to date? | VP of Administration |
| Which function in your organization approves security policies and procedures? | VP of Administration |
| Are there provisions for disciplinary actions for non-compliance with policies and procedures? | Yes |
| Does your organization communicate changes within policies and procedures to the staff? | Yes |
| Who is in the scope of communication? | All employees, contractors and temporary workers (if any). |
| How are changes within policies communicated? | Via data security and privacy policies handbook verbal instruction |
| Does your organization have a formal (documented, approved, published, communicated and implemented) process in place to approve exceptions to policies? | No, no policy exceptions are permitted |
| | |
| **4 - Organizational Security** | |
| How is senior management commitment to information security demonstrated? | The President and CEO review and approve all data privacy and security policies |
| Does your organization have an Information Security Oversight function? | Yes |
| Does this function receive full required support from senior management? | Yes |

| | |
|---|---|
| Does the function have responsibility for consistent implementation of information security across different parts of your organization? | Yes |
| Does your organization perform internal security audits on a regular basis? | Yes |
| Which function is responsible for performing internal security audits? | VP of Administration |
| How is senior management notified about internal security audit results? | They participate in the audit process |
| When was the last time an internal security audit was completed? | January 2022 |
| Does your organization have any industry-standard independent attestations to support the services which you already provide or will be providing? | Yes, our hosting service provider (Azure) provides ISO270001, ISO270018, SOC2, etc. |
| Is your organization required to comply with any legal, regulatory or industry requirements? | No |
| | |
| **5 - Human Resource Security** | |
| Do all applicants for employment (including internal staff and external individuals such as consultants, contractors and employees of third parties) complete an employment screening process? | Yes |
| What is the scope of the employment screening process? | Identity check<br>Criminal Record Check |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | |
|---|---|
| | Credit Check<br>Employment History |
| Does your organization require the employment screening process to be completed before commencing any kind of employment? | Yes |
| On what basis does your organization repeat the screening process of an individual? | If individual requires a higher privilege level |
| What is your procedure should an individual fail the repeat screening process? | Individual does not receive the higher privilege level and their current privilege level is reviewed |
| Please list all documents that an individual needs to sign before commencing any kind of employment. | Employment Contract<br>Code of Ethics<br>Non-Disclosure Agreement<br>Acceptable Use |
| Does your organization have a formal (documented, approved, published, communicated and implemented) security awareness program and associated training policy? | Yes |
| How often are the security awareness sessions conducted? | Yearly |
| Are security awareness sessions mandatory for all employees? | Yes |
| How does your organization track attendance to the security awareness session? | Manually |
| Does your organization perform regular clean desk checks? | Yes |

| | |
|---|---|
| Are those checks performed on random/surprise basis? | Yes |
| | |
| **6-1 - Physical and Environmental Security - office locations** | |
| What physical controls are utilized within your organization's office locations? | Manned reception desk<br>CCTV<br>Metal keys<br>Smoke/fire alarm |
| Does your company ensure that critical systems and applications are protected from external and environmental threats? | Yes |
| Describe how it is ensured | All critical systems and applications are hosted in secure environments. |
| How will continuity of service be ensured in case of a power failure? | All critical systems and applications can be accessed in backup locations in case of power failures. |
| How will continuity of service be ensured in case of a network failure? | All critical systems and applications can be accessed by alternate networks in the event of a failure. |
| How will continuity of service be ensured in case of a hardware failure? | All critical systems and applications can be accessed by backup hardware. |
| Does your organization ensure that only authorized personnel have access to office premises? | Yes |
| Describe how it is ensured | Access to office premises is managed by VP of Administration and building manager |

| | |
|---|---|
| Is access to office premises granted on "need-to-know"/"need-to-have" basis? | Yes |
| Are all entries recorded? | Yes |
| Does your organization have process of periodic physical access review? | Yes |
| Describe this process | Building manager and VP of Administration review physical office access keys regularly. |
| Is there a formal visitors policy in place? | No, but we rarely receive visitors at our business office. The ones we do receive are previously known and are escorted at all times. |
| Is there an emergency access / exit (e.g. emergency access door) process in place? | Yes |
| | |
| **6-2 - Physical and Environmental Security - Data Center** | |
| Does your organization use any Data Centers that are not main office location, for hosting/processing data? | Yes |
| What type of hosting services does your organization utilize? | We currently use a dedicated server hosted by Microsoft Azure cloud server. |
| What physical controls are utilized within Data Center locations? | Card controlled entry gates<br>Manned reception desks<br>Security guards<br>CCTV<br>Security control room |

| | |
|---|---|
| | Burglary proofed doors/windows<br>Electronic access devices with PIN<br>Bio-metric access devices<br>Open door alarm<br>Smoke/fire alarm |
| Does your company ensure that critical systems and applications are protected from external and environmental threats? | Yes |
| How will continuity of service be ensured in case of a power failure? | Auxiliary power. |
| How will continuity of service be ensured in case of a network failure? | Auxiliary network connection. |
| How will continuity of service be ensured in case of a hardware failure? | Cloud based servers. |
| Does your organization ensure that only authorized personnel have access to a Data Center location? | Yes via the hosting services provider |
| Does your organization perform periodic physical access reviews? | Yes, by the hosting services provider |
| Is there a formal visitors policy in place? | Yes |
| Are all visitors required to provide government issued ID? | Yes |
| Are all visitors signed in / logged? | Yes |
| Are all visitors escorted at all times and required to wear clearly identifiable visitor credentials? | Yes |

| | |
|---|---|
| Is there an emergency access / exit (e.g. emergency access door) process in place? | Yes |
| | |
| **7 - IT Asset Management** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Asset Management policy? | Yes, in the Data Security and Privacy Handbook |
| Does your organization identify and record all applications, systems and IT infrastructure components in a central asset inventory? | Yes |
| How does your organization identify and monitor software which is out of support? | Via input from hosting service, security staff and development staff. |
| Does your organization have a list of approved software/hardware which is the only software/hardware that can be used (whitelisting)? | Yes |
| Does your organization have a process for maintaining up-to-date network documentation (e.g. network diagrams)? | Yes |
| Describe this process | When the network is updated we request an updated network diagram from our network security specialist. |
| Does your organization use any End Use Applications (EUAs)? | No |
| Does your organization record and manage all software license agreements in a central repository? | Yes |

| | |
|---|---|
| How does your organization monitor compliance and expiration of software license agreements? | VP of Administration monitors. |
| What information regarding software license agreements is recorded in the central repository? | Software version<br>Software location<br>License expiry date<br>Licensing requirements |
| Does your organization utilize a data classification system? | Yes |
| Does your organization ensure that confidential data is secured during maintenance service (e.g. hard-drive failure, server malfunction)? | Yes |
| Describe how it is ensured | All confidential data is secured by our hosting service provider and they have internal policies for maintenance service. |
| Does your organization have any physical records (e.g. paper documents, microfiche) which contain customer data? | No |
| Does removable storage media (e.g. USB, CD/DVD) containing customer data ever leave your organization's premises? | No |
| How does your organization dispose of electronic media (e.g. hard-drives, USB sticks, CD's / DVD's)? | We do not use local hard-drives, USB sticks, CDs or DVD to store confidential data. Server hard drives are disposed of by Azure according to industry best practices. |
| Who is accountable for information disposal? | VP of Administration |

| | |
|---|---|
| How does your organization guarantee the disposal of removable storage media? | The hard drives of obsolete machines are wiped prior to disposal |
| How does your organization ensure that all assets (e.g. laptops, mobile phones) have been returned upon termination? | VP of Administration tracks |
| | |
| **8 - System Access Control** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Access Management policy? | Yes. This is included in the Data Privacy and Security Handbook. |
| Does your organization document all system access rights and roles? | Yes |
| How does your organization document all access rights and roles? | We are a small organization so there is a very small number of users that have access rights. This is tracked by VP of Administration. |
| Does your organization include usage flags to restrict access rights / role descriptions to certain types of users? | Yes, the StockOpter application has user levels. |
| Do access rights/roles descriptions explain what kind of access the user has (read, write, modify, etc.)? | Yes |
| Who is responsible for creating and maintaining role descriptions within your organization? | VP of Administration |
| Does your organization have the access management process in place? | Yes |

| | |
|---|---|
| Describe the access management process that is followed in your organization (what verification is done, what approvals need to be collected). | The need for access is verified and approved by the VP of Administration. |
| Does your process ensure separation of access from development/testing environment and production? | Yes |
| Describe how it is ensured | StockOpter.com has separate development, test/quality and production environments. All modifications to the system are coordinated by the CEO as follows:<br>Code changes are specified in writing to a programmer. The programmer develops the code on the development system. When it is ready for testing the programmer promotes the codes to the Test/QA environment. Development & testing are iterative, so it usually takes several cycles to perfect the modification. Upon completion of testing, the code is promoted to the production system by the development team. A final test of the modification is done on the production system. |
| Does your process ensure segregation of duties to prevent unauthorized manipulation of identities and user access rights? | Yes |
| Does your process ensure toxic combinations are identified and managed appropriately? | Yes |
| Does your organization review the access rights of (internal and external) employees? | Yes |
| How often is the access rights review performed? | Quarterly |

| | |
|---|---|
| Are "need-to-know" and "need-to-have" principles considered when access is requested? | Yes |
| Does your organization have a process of provisioning temporary emergency access (break glass process)? | No, it has not be necessary |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Joiner/ Movers / Leavers policy? | Yes |
| Does your organization have a formal account creation process for new joiners? | Yes |
| Describe this process | Once employee is vetted, a user id is created with the appropriate access level to perform their job created by the VP of Administration |
| Does your organization ensure that access entitlements are adjusted for a change in internal status (mover)? | Yes, by VP of Administration and adjustments are made immediately. |
| How does your organization ensure that access entitlements are revoked upon termination of an employment contract or agreement (leaver)? | Access for a terminated employee is disabled immediately by the VP of Administration |
| Are non-personalized technical accounts (e.g. non-human accounts such as service, communication, application and database accounts) assigned to respective application/service owner? | Yes |
| How does your organization ensure that technical accounts have rights assigned on least privileged basis? | We review the accounts used by all services (including the identity of each IIS app pool), taking care to ensure that all services are using least privileged and named accounts |

| | |
|---|---|
| | as appropriate. In no event would we ever stipulate the identity of an app pool as a system administrator. |
| How does your organization manage passwords to technical accounts? | Technical account passwords are system generated and managed by the VP of Administration |
| How does your organization ensure that product/application default accounts are disabled or at least passwords to them are changed? | In accordance with our IT risk management policy, no applications or services may be installed or configured which create default accounts, beyond operating system service accounts and groups. |
| Does your organization separate (physically or logically) staff working on specific customer data from the rest of your employees? | No, we are a small shop |
| Does your organization implement a formal (documented, approved, published, communicated and implemented) Password policy? | Yes |
| Is Password History enforced? | Yes |
| What is the Password History set? | Last 6 passwords. |
| Is Minimum Password Age set? | Yes |
| Is Maximum Password Age set? | Yes |
| What is the Maximum Password Age set? | 90 days |
| Is Minimum Password Length set? | Yes |
| What is Minimum Password Length set? | 8 |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | |
|---|---|
| Is Password Complexity enforced? | Yes |
| Describe Password Complexity requirements used | Requires: upper, lower, number, special character and can't include user name. |
| Does your organization utilize multi-factor authentication? | No |
| How does your organization prevent employees from connecting personally owned mobile computing or storage devices to any system or network which may be involved in the processing or storage of customer information? | Customer data is not stored on any local devices. Customer data is only stored at our secure data center, which employees cannot physically access. |
| Does your organization allow employees to remotely connect to your internal network (e.g. working from a non-office location)? | No, we don’t utilize an internal network |
| Describe the process of granting remote access. | Only our developer can establish a VPN connection to our server to perform maintenance |
| How many employees have remote access to customer data? | 0 |
| Is split tunneling prohibited? | No |
| Is it possible to save data on a local drive during remote connections? | No |
| Is remote printing disabled? | Yes |
| Does your organization allow users to work remotely from private laptops / desktops? | No, corporate devices only |

| | |
|---|---|
| Are you aware of any reason why your organization would need to implement any cross-border restriction requirements to prevent prohibited geographical exchanges of data? | No |
| | |
| **8-1 - Separation of environments** | |
| Does your organization separate environments from each other (development, test, production)? | Yes |
| Describe how it is ensured | By policy managed by VP of Administration |
| How does your organization ensure that development tools (including compilers) are not installed within the production environment? | By policy managed by VP of Administration |
| How does your organization ensure that program source code libraries held in production systems, can only be read-accessed by developers? | By policy managed by VP of Administration |
| Does your organization utilize production data for test or/and development purposes? | No |
| | |
| **9 - Network Security** | |
| What network security controls has your organization implemented? | Firewalls |

| | |
|---|---|
| Does your organization monitor network traffic and system activities? | Yes |
| How does your organization monitor network traffic? | Azure Security Center provides IDS and IPS including DDOS and related monitoring |
| How does your organization monitor system activities? | Through the Azure Portal, including the Azure Security Center's event log monitoring. |
| What type of intrusion detection/prevention software (IDS/IPS) is utilized within your organization? | Network Intrusion Detection System<br>Network Intrusion Prevention System<br>Host Intrusion Detection System<br>Host Intrusion Prevention System<br><br>Azure VM agents and endpoint protection are installed on all Azure VMs, covering all of the above. |
| Please describe the process which is followed in your organization in case of anomaly detection | In the event of intrusion or other issues, system administrators are notified immediately. The IT response will vary based on the anomaly detected. |
| Is wireless technology used within your organization? | No |
| | |
| **10 - Security Monitoring and Logging** | |
| Is Anti-Malware software installed on all your organizations' servers, desktops, notebooks and mobile end user devices? | Yes |
| How does your organization ensure that Anti-Malware is installed and active on all devices? | Managed by VP of Administration |

# Net Worth Strategies – StockOpter.com Security Questionnaire

August 2022

| | |
|---|---|
| Is Anti-Malware software centrally managed? | Yes |
| How often are malware signatures updated? | Daily |
| Has your organization deployed a comprehensive Data Leakage Prevention (DLP) program to detect or prevent the loss of confidential client data through data leakage? | No, this is done manually because we're a small company |
| Does your organization scan for unauthorized software? | Yes |
| What actions are taken when unauthorized software is found? | It is immediately removed. |
| Does your organization capture security logs from systems and devices? | Yes |
| Please explain details of the security monitoring process. | Our solution will be deployed and managed with Microsoft Azure. We will utilize Azure Log Integration to analyze all system event and activity logs, which reflect any issues through the Azure Security Center portal. The portal is configured to notify our system administrators immediately if any issues occur. |
| What routines, events and activities are logged? | All operating system, application, security, setup, and other ancillary server events and activities are logged on all servers. |
| Which information is included in the log file? | Alert/event level, date and time, service or system source, event ID, category, user or identity running the process, and host name. |

| | |
|---|---|
| What is the security log retention period? | Security logs are kept for 90 days |
| Where are the logs stored? | Logs are stored locally on each server and are integrated and exported to the Azure Security Center continually. |
| How does your organization protect the logs from alteration? | Windows ACL provides event log security on our VMs, beyond which logs are shipped to the Azure Security Center. Administrative access and permissions are limited and monitored, further preventing log tampering. |
| Please describe how segregation of duties is enforced in logging and monitoring activities. | The software deployment team has access to the build service which deploys system updates to our VMs as needed. The system architect has further access to the virtual machines should an issue arise. The system architect does not have access to the security portal, which is owned and managed by the operations division. Because logs are shipped, no one team could effectively manipulate all log files. |
| | |
| **11 - Vulnerability and Threat Management** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) vulnerability scanning program in place? | Yes |
| Please indicate which systems are in scope of vulnerability scans | Systems and their available network-based communication ports |
| What is the scope of the vulnerability scan performed? | All open TCP and UDP ports are tested and logged on a quarterly basis. SSL certificates are also tested and |

| | |
|---|---|
| | reviewed. Full penetration tests can be provided or facilitated upon request, though additional fees may apply. |
| How often is the scope/configuration of the vulnerability scanning reviewed? | Quarterly |
| How often are vulnerability scans performed? | Quarterly |
| Is the remediation of security weaknesses monitored and reported to a respective security function? | Yes, security issues are automatically reported to our VP of Admin. Remediation of said weaknesses are overseen by them as well. |
| What is the time-frame for fixing Critical, Major, Moderate, Minor and Non-significant vulnerabilities? | Critical and major security vulnerabilities are addressed immediately (within hours). Moderate and minor are addressed within 2-3 business days. Non-significant vulnerabilities are addressed during scheduled updates. |
| Are vulnerability scans performed by a third party company? | Yes |
| Which company does your organization utilize for this purpose? | Our contract security specialist performs the vulnerability scans. |
| Does your organization have a formal (documented, approved, published, communicated and implemented) penetration testing program in place? | No, but we conduct ad hoc static and dynamic penetration tests for a fee based on customer requests. These services have been provided by a variety of providers over the years but most recently we have used BreachLock. |
| Does your organization have a process of managing external and internal sources of IT security threats? | Yes |

| | |
|---|---|
| How does your organization identify threats that are applicable to your operating environment? | We have documented processes and procedures in place for identifying and responding to potential threats. We have a contract security specialist review our processes and procedures, providing updates as appropriate. |
| How does your organization ensure that list of applicable external and internal sources of IT security threats is up-to-date? | We communicate regularly with our contract security specialist to keep abreast of new threats as they occur. |
| | |
| **12 - Cryptographic Controls** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Cryptographic policy and standard? | Yes |
| Does your organization encrypt data at rest? | Yes |
| Please provide information about cryptography controls used for encryption for data at rest. | Personal computers have disk encryption software. |
| How does your organization encrypt data on mobile computers such as laptops? | Symantec Encryption software. |
| What symmetric cryptography algorithms does your organization use? | AES-256 |
| Does your organization encrypt data in transit? | Yes |
| Please provide information about cryptography controls used for encryption for data in transit. | We use the current versions of TLS. |

| | |
|---|---|
| Which SSL/TLS versions does your organization use? | TLS 1.2 |
| What asymmetric cryptography algorithms does your organization use? | RSA-2048 |
| Provide details regarding encryption key management. | Managed by VP of Administration |
| Does your organization use hashing? | Yes |
| For what purposes are hash functions used? | Passwords |
| What hash algorithms does your organization use? | SHA-256 (SHA-2 family) |
| Does your organization use encryption mechanism for remote connections? | Yes |
| What encryption technologies does your organization use? | Secure Sockets Layer (SSL) |
| | |
| **13 - Change and Release Control** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Change Management policy? | Yes |
| Does your organization ensure that system components and software have the latest vendor-supplied security patches installed? | Yes |

| | |
|---|---|
| Explain what the process is for the deployment of system and software patches. | Handled by hosting provider and security specialist. |
| Does your organization utilize a central patch repository distribution solution? | Yes |
| What is the timeframe to patch unpatched systems? | Daily |
| Are remediation of unpatched systems monitored and reported to respective security function? | Yes |
| Does your organization have a formal (documented, approved, published, communicated and implemented) emergency fix process? | Yes |
| | |
| **14 - Software and Hardware Hardening** | |
| Does your organization use standard, formally approved builds for systems? | No |
| Does your organization harden network, server devices and workstations (particularly those which process, store or view customer information) prior to installation and use? | Yes |
| Describe this process | Per prior responses regarding software installation procedures, we harden our network, server devices, and workstations by changing all default passwords, enforcing password change and complexity policies, disabling all unnecessary software and services, isolating VLANs, isolating endpoints, having a multitier topology, and |

| | |
|---|---|
| | having robust firewalls and intrusion-prevention with logging and alerting. |
| What industry best practices does your organization follow? | PCI DSS security standards are followed. |
| | |
| **15 - BCM and IT Disaster Recovery** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Business Continuity / Disaster Recovery (BC/DR) policy? | Yes |
| What does your organization's BC/DR identify? | Key tasks<br>Key applications<br>Key dependencies |
| Does your Business Continuity/ Disaster Recovery plan have a plan owner and a deputy assigned? | Yes |
| Is your organization's Business Continuity/ Disaster Recovery signed-off by the plan owner? | Yes |
| How it is ensured that BC/DR plan owner or deputy have sufficient authority to execute the plan during a crisis? | VP of Administration is ultimately responsible. |
| How often is your organization's BC/DR plan reviewed? | Yearly |
| Does your organization's BC/DR plan have a process defined to contact all recovery staff? | Yes |

| | |
|---|---|
| Does your organization perform a periodic test of the BC/DR plan? | Yes |
| What types of testing does your organization perform? | Checklist Test<br>Structured Walk-Through Test |
| How often is the plan tested? | Every six months |
| When was the last test performed? | May 2022 |
| Does your organization document results of the tests? | No |
| How does your organization ensure that BC/DR plans are updated with relevant lessons learned from the tests? | An update to the Data Privacy/Security Handbook |
| | |
| **16 - Data Backup & Recovery** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) process to perform regular backups of essential information, software and/or infrastructure configuration? | Yes, managed by Azure |
| How are data backup requirements for essential information, software and/or infrastructure configuration documented? | Backups are run daily and stored on-site by our third-party hosting site, Microsoft Azure. |
| Do applicable owners review and validate backup requirements periodically? | Yes |

| | |
|---|---|
| How often are they reviewed? | Yearly |
| How is the completeness of backup requirements monitored and any deficiencies/outstanding validations reported? | By our hosting provider, Microsoft Azure |
| Where does your organization store data backups? | Externally |
| What media does your organization utilize for information backup? | Tape |
| How does your organization ensure safe transportation of backup media? | Provided by hosting service provider |
| Is backup data encrypted? | Per Azure's protocols |
| Does your organization test backup data and system restoration procedures? | Yes |
| What is the scope of backup data and system restoration testing? | Testing of backup agreements with external vendors and critical suppliers |
| Which system restoration procedures are utilized within your organization? | Recovery routines |
| How often does your organization test data and system restoration procedures? | Monthly |
| How does your organization dispose of backup media? | Per Azure's protocols |
| Who is accountable for backup disposal? | Microsoft Azure |

| | |
|---|---|
| How does your organization guarantee the disposal of all backup data? | Azure guarantees. |
| | |
| **17 - Incident and Problem Management** | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) Information Security Incident Management policy? | Yes, it is included in the Data Privacy and Security Handbook. |
| What is the scope of the information security incident management process? | Our security incident management process incorporates all security events ranging from monitoring and responding to active data intrusion detection to responding to desktop security incidents. The scope of our incident management process therefore is comprehensive for our organization |
| Which elements/steps are included in the information security incident management process? | Incident identification<br>Incident response<br>Recovery<br>Post-incident review |
| Are all security incidents handled within a centralized ticket based incident management system? | Yes |
| What information is included in a security incident ticket? | Date, time, type, scope, duration, applications/networks affected, etc. |
| Does your organization perform an impact assessment on each security incident? | Yes |

| | |
|---|---|
| Describe this process | There have been no security breaches to date but security incidents will be assessed for impact by our security specialist and hosting service. |
| How does your organization ensure that evidence is preserved for forensic investigations/purposes? | We will be using Microsoft Azure's security center. |
| Does your information security incident management process include criteria of when clients should be notified in the event of an incident? | Yes |
| What is the criteria for notifying customers in the event of a security incident? | Evidence that their customer data has been compromised. |
| Does your organization perform periodic formal reviews of the information security incident management process? | No, it hasn't been necessary |
| | |
| **18 - Data Integrity** | |
| Does your organization monitor system and application jobs, batches, processes and tasks to detect and address correct sequencing, data processing failures and deviations from scheduled processing? | Yes |
| Describe this process | Application jobs are run nightly and the results of these processes are checked by the support staff for correctness and failures. |
| | |

| | |
|---|---|
| **19 - Archive Management** | |
| How does your organization ensure that all archive records are stored for the minimum period of time as defined by applicable regulatory laws? | The StockOpter application archives all customer client reports indefinitely. |
| How does your organization ensure that only persons with legitimate reasons have access to archived records? | VP of Administration limits archived report access to essential personnel only. |
| Does your organization check that all records arrive at the archive as expected? | Yes |
| Does your organization ensure that records are purged from the archive system after the minimum period of time defined by applicable regulatory laws? | No<br><br>Archived data and client reports are currently kept indefinitely for legal defense purposes. |
| | |
| **20 - Capacity Planning and Performance Management** | |
| Does your organization ensure that systems are designed with sufficient capacity to cope with expected information processing requirements? | Yes |
| Describe how it is ensured | With Microsoft Azure where we can increase capacity on the fly. |
| Does your organization conduct performance and capacity forecasting of IT resources? | No |

| | |
|---|---|
| Does your organization continuously monitor the capacity, performance and availability of IT resources? | Yes |
| Does your organization monitor changes in the business which would impact system or application capacity? | Yes |
| Please describe this process | The CEO constantly monitors business and usage volumes that would impact system and application capacity. |
| How are such changes communicated to the respective system/application owner? | The CEO is the application owner so communication is seamless. |
| | |
| ********** **Service Level Controls** ********** | |
| | |
| **22 - Software services – hosted on non-customer Infrastructure** | |
| Is the software that is in scope of this assessment developed specifically for any customer? | No |
| Is the software that is in scope of this assessment a Commercial Off-the-Shelf product? | Yes |
| Is the Commercial Off-the-Shelf software that is in scope of this assessment customized specifically for any customer? | No |
| Does your organization have a formal (documented, approved, published, communicated and | Yes |

| | |
|---|---|
| implemented) Secure Software Development Lifecycle (SSDLC) that is followed for each software development project? | |
| Are industry best practices including processes, methods, tools, and techniques used to produce or change the software that is in scope of this assessment? | Yes |
| Please describe applicable industry best practices. | The StockOpter.com application uses .NET / IIS technology standards within SSDLC. |
| Does your organization have a formal (documented, approved, published, communicated and implemented) change management process for software development project? | Yes |
| Please describe the process. | StockOpter.com has separate development, test/quality and production environments. All modifications to the system are coordinated by the VP of Operations as follows:<br>1.Code changes are specified in writing to a programmer<br>2.The programmer develops the code on the development system<br>3.When it is ready for testing the programmer promotes the codes to the Test/QA environment<br>4.Development & testing are iterative, so it usually takes several cycles to perfect the modification<br>5.Upon completion of testing, the code is promoted to the production system by the development team<br>6.A final test of the modification is done on the production system |

| | |
|---|---|
| Has the software been evaluated against the Common Criteria, FIPS 140-2, or other formal evaluation process? | No |
| Does your organization provide support for the software that is in scope of this assessment? | Yes |
| Please provide the scope of the support provided | We respond immediately to any and all StockOpter.com user issues and we automatically track system errors. |
| Please describe how your organization is notified when support is necessary | By email (stockopter@networthstrategies.com) or phone (541-383-3899) |
| How is the support executed? | By customer support personnel. |
| Is support executed or possible to be executed via remote connection from a non-office location? | No |
| Is the software that is in scope of this assessment a web-based application? | Yes |
| What is the URL (web) address of the software? | https://app.stockopter.com/ |
| Does your organization offer this software to other clients? | Yes |
| How is customer data separated from other clients data? | Logical separation within the same multi-tenant database |
| If customer data resides in a multi-tenant database, what technical controls and assurance measures are taken to ensure absolute isolation of that data with respect to other clients' access privileges? | Yes<br><br>SQL Server technical controls. |

| | | |
|---|---|---|
| If customer data resides in a multi-tenant database, do customers have an option to use a dedicated database instead? | Not currently | |
| If customer data resides on the same machine as other clients, do customers have an option to use a dedicated machine? | Yes | |
| Please describe software architecture (please attach software architecture diagram) | 3 Tier .NET application that uses SQL server. | Network Diagram - Azure.png |
| Who are the users of the web-based application that is in scope of this assessment? | Customer employees | |
| How many people from your organization have access to customer data through the web-based application, and what are their roles? | 3: CEO, VP of Administration | |
| How many people from your organization have access to the database where customer data is stored, and what are their roles? | 2: Security specialist. Developer. | |
| Is it possible to remotely access the database where customer data is stored from non-office location? | No | |
| Does your organization have a formal (documented, approved, published, communicated and implemented) process for managing access to the web-based application? | Yes | |
| How does a user request access to the web-based application? | Customer admin users control user access requests. | |
| Who approves the request? | Customer admin account contact | |

| | |
|---|---|
| How is access granted? | Customer admin account contact |
| How is access revoked? | Customer admin account contact |
| Are customers periodically informed about all users who have access to the web-based application in scope of this assessment? | No, system administrators can view this data at any time. |
| Is the web-based application compliant with your organizational Password Policy? | Yes |
| How is a new user informed of their initial password to the web-based application? | Via automated email. |
| Does the password need to be changed upon first login? | Yes |
| For what period of time is the initial password valid? | 2 days. |
| Please describe the process of resetting a password. | General users can use the "Forgot Password" function.<br>Admin users can reset passwords for general users. |
| Where are the passwords to the web-based application stored? | In the SQL database |
| How does your organization protect users' passwords for the web-based application that is in scope of this assessment? | Salted signature hash |
| Does the web-based application support multifactor authentication? | No, not yet |
| Is Web Single Sign On implemented for the web-application that is in scope of this assessment? | No |

| | | |
|---|---|---|
| Does the web-based application support SAML 2.0? | No | |
| Is access to the web-based application for customer users restricted to the customer network only - customer IP address whitelisting is applied? | No, but IP address whitelisting can be applied upon request. | |
| Does the web-based application compliant with your organizational requirements for Penetration Testing? | Yes | |
| Have the web-based application ever been penetration tested? | Yes | |
| When was the last penetration test performed? | May 2021 | |
| What were the results of the last penetration test? (please attach the penetration test report) | 2 high and 4 medium issues were identified and remediated. | StockOpter.com_Pentest_Summary_Report_05-8-2015.docx |
| Have all identified findings been remediated? | Yes | |
| Does the web-based application compliant with your organizational requirements for Vulnerability Scanning? | Yes | |
| How often does your organization perform URL-based vulnerability scanning for the web-based application? | Quarterly | |
| How often does your organization perform IP-address-based vulnerability scanning for | Quarterly | |

| | |
|---|---|
| infrastructure underlying the web-based application? | |
| Is SSL/TLS utilized to secure the web-based application? | Yes |
| Which SSL/TLS versions are enabled? | TLS 1.2 |
| Which cipher suits are enabled? | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256<br>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256<br>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384<br>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256<br>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384<br>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256<br>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 |
| Does your organization utilize an external Certificate Authority (CA) to sign the application certificate? | Yes |
| Which Certificate Authority (CA) signs the application certificate? | The SSL certificate is an RSA 2048 bit certificate issued by Sectigo's secure CA. |
| Does your organization use a Hardware Security Module (HSM) to protect the application certificate? | No |
| How does your organization protect the application certificate? | The only certificate we use is an RSA-2048 SSL certificate installed in our IIS web server. It is not stored on individual desktops or otherwise in our LAN. |
| Does your organization utilize a web firewall to protect the web-based application that is in scope of this assessment? | Yes |

| | |
|---|---|
| Is the backup of the software in scope of this assessment compliant with your organizational backup procedure? | Yes |
| How often is the backup of the software performed? | Daily |
| What is RTO (Recovery Time Objective) for the software? | 24 hours |
| What is RPO (Recovery Point Objective) for the software? | 24 hours |
| Does your organization deploy any protection against DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks? | Provided by Azure |
| Is the software that is in scope of this assessment a client-server application? | No |
| Does your organization separate (physically or logically) staff working on customer data from the rest of your employees? | No because we are a small company and have many customers. |