Policy Title:	Interoptex Information Security Policy
Date of Issue:	6/14/17
Version:	1.6
Document Owner:	Seth Hobgood
Document Purpose:	To detail Interoptex's high-level Information Security Policies.

Version	Date Issued	Brief Summary of Change	Approver Name
V1.0	2/27/15	Creation	Seth Hobgood
V1.2	9/11/15	Added Security Reminders to 5.22	"
V1.3	3/8/16	Added BYOD	"
V1.4	6/14/17	Annual Revision, added Network Pen Test	Seth Hobgood
V1.5	2/14/2018	Added Cybersecurity NIST References, HITRUST Mappings	Seth Hobgood
V1.6	10/8	Added public access via site	Mark Thienel

1. Introduction

This top-level information security policy is a key component of Interoptex's overall information security management framework and should be considered alongside more detailed information security documentation including, system level security policies, security guidance and protocols or procedures. Interoptex's vendor partners are expected to be in compliance with the requirements of this policy. Interoptex will routinely evaluate the IS policies and procedures of vendor partners to ensure both entities' internal security policies are aligned.

The CTO or a designee of the CTO (typically a network administrator or Manager of IT) will ensure the following policy and procedure requirements are in place. This individual is responsible for ensuring implementation of any of the following criteria beginning with the phrase 'Interoptex will', 'Interoptex uses', or other such phrasing unless more specific language is used.

All employees are required to sign off on this policy annually to ensure they are aware of the company's information security goals. Interoptex will facilitate the completion of this documentation during the annual HIPAA security training session.

Interoptex ensures that communication protection requirements, including the security of exchanges of information, is the subject of policy development and compliance audits.

(HITRUST 0113.04a1Organizational.123), (HITRUST 0914.09s1Organizational.6), (HITRUST 0178.05h1Organizational.3)

2. Objectives, Aim and Scope (HITRUST 1324.07c1Organizational.3)

2.1. Objectives

The objectives of Interoptex's Information Security Policy are to preserve:

- **Confidentiality** - Access to Data shall be confined to those with appropriate authority.
- **Integrity** – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification. Covered information in storage will be kept to the minimum required to execute business operations and will only be stored in specified locations. (HITRUST 19242.06d1Organizational.14, 19243.06d1Organizational.15)

- **Availability** - Information shall be available and delivered to the right person, at the time when it is needed. (HITRUST 0113.04a1Organizational.123)

2.2. Policy Aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by Interoptex. The CTO or most senior technical resource within the organization will ensure the following practices are applied:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principals of security and explaining how they shall be implemented in the organization.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organization a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organization. (HITRUST 0102.00a2Organizational.123)

2.3. Scope

This policy applies to all information, information systems, networks, applications, locations and users of Interoptex's systems or supplied under contract to it.

3. Responsibilities for Information Security (HITRUST 0104.02a1Organizational.12)

3.1. Ultimate responsibility for information security rests with the Chief Executive Officer of Interoptex but on a day-to-day basis the Engineering lead shall be responsible for managing and implementing the policy and related procedures.

3.2. Department heads are responsible for ensuring that their permanent and temporary staff and contractors are aware of: -

- The information security policies applicable in their work areas
- Their personal responsibilities for information security
- How to access advice on information security matters

3.3. All staff shall comply with information security procedures including the maintenance of data confidentiality and data integrity. Failure to do so may result in disciplinary action.

3.4. The Information Security Policy and all other security policies shall be maintained, reviewed and updated by the company officers and/or security team based on NIST Cybersecurity framework version 1.0. Approval from one member of this team is required for updates to this policy. These reviews shall take place annually. (HITRUST 0114.04b1Organizational.1)

3.5. The Information Security Policy shall be made available to the public via Advent's web site. (HITRUST 1862.08d1Organizational.3)

3.6. Department heads shall be individually responsible for the security of their physical environments where information is processed or stored in accordance with the "Facility Access Controls" policy.

3.7. Each member of staff shall be responsible for the operational security of the information systems they use.

3.8. Each system user shall comply with the security requirements that are currently in force, and shall also ensure that the confidentiality, integrity and availability of the information they use is maintained to the highest standard.

3.9. Contracts with external organizations that allow access to Interoptex's information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organization shall comply with all appropriate security policies.

3.10. Data protection will be enforced according to NIST Cybersecurity framework version 1.0. (HITRUST 0101.00a1Organizational.123)

3.11. A company officer must be designated as the Security Officer and detailed at the bottom of this policy. (HITRUST 0117.05a1Organizational.1)

4. Legislation

4.1. Interoptex is obliged to abide by all relevant legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the Interoptex, who may be held personally accountable for any breaches of information security for which they may be held responsible. Interoptex shall comply with all applicable state and federal legislation.

5. Policy Framework

5.1. Employee Management of Security

- At executive level, responsibility for Information Security shall reside with the Security Officer.
- The Security Officer shall be responsible for implementing, monitoring, documenting and communicating security requirements for the organization.
- Employees that do not comply with the details of this policy and its child policies may be subject to disciplinary action, up to and including termination.
- Security issues noticed by employees should be immediately escalated to their immediate supervisor, who should then notify the Security Incident Response Team via the helpdesk. Further details for PHI-related security incidents are defined in the 'Security Incident Response and Management Policy'. (HITRUST 0135.02f1Organizational.56)
- Employees may initiate complaints on, requests to update, or records regarding the disposition of this and other security policies by contacting the helpdesk. (HITRUST 0162.04b1Organizational.2)
- For more information on the general handling of PHI refer to the company's Data Integrity policy.

5.2. Contracts of Employment

- Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.
- Information security expectations of staff shall be included within appropriate job definitions.

5.3. Security Control of Assets

Each IT asset, (hardware, software, application or data) shall be inventoried and tracked per Interoptex's "*Device and Media Control*" policy.

5.4. Access Controls

Only authorized personnel who have a justified and approved business need shall be given access to restricted areas containing information systems or stored data per the "*Access Control*" policy.

5.5. User Access Controls

Access to information shall be restricted to authorized users who have a legitimate business need to access the information pre the "*Access Control*" policy.

5.6. Application Access Control

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorized users who have a legitimate business need e.g. systems or database administrators. Authorization to use an application shall depend on the availability of a license from the supplier.

5.7. Equipment Security

In order to minimize loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards. All server and networking components will be located behind doors requiring badged access. Appropriate care should be taken to physically protect any laptops or other mobile assets that leave the premises. See the "*Workstation Use and Security*" policy for further details.

5.8. Computer and Network Procedures

Management of computers and networks shall be controlled through standard documented procedures that have been authorized by the network or IT manager.

Interoptex has a network protection plan that ensures the following tenets are applied to company networks:

- Interfaces will deny by default
- Access will require explicit identification
- Systems will have their level of sensitivity documented
- Logical and physical network separation will be applied to maintain minimum necessary levels of access
- Up-to-date network diagrams will be maintained detailing all network devices and will be updated with any changes, with updates occurring no less often than every six months. The network or IT manager will maintain this diagram.

(HITRUST 0894.01m2Organizational.7, 0819.09m1Organizational.23)

5.9. Information Risk Assessment

Once identified, information security risks shall be managed on a formal basis. They shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed as needed. These reviews shall help identify areas of continuing best practice and possible weakness, as well as potential risks that may have arisen since the last review was completed.

A recurring meeting will be held with all department heads to review outstanding IT/IS issues and discussion of known or perceived risks. More details can be found in the "*Risk Analysis and Management*" policy.
HITRUST1412.09f2System.12

5.10. Information security events and weaknesses

All information security events and suspected weaknesses are to be reported to the Engineering lead or Systems Administrator. All information security events shall be investigated to establish their cause and impacts with a view to avoiding similar events. More details can be found in the "*Incident Management*" policy.

5.11. Classification of Sensitive Information.

Interoptex shall implement appropriate information classifications controls, based upon the results of formal risk assessment.

The classification **PHI** shall be used for patients' clinical records, patient identifiable clinical information passing between Interoptex staff and between other appropriate agencies. All PHI shall be handled in a sensitive manner and according to HIPAA regulations and the systems detailed in Interoptex's PHI Incident Management Policy. Although not technically termed PHI, credit card information will be handled with the same restrictions and sensitivity as PHI.

In order to safeguard confidentiality, any internal documents termed "Confidential" shall **not** be distributed to any individuals or channels outside of the Interoptex customer base or contracted vendor partners.

5.12. Protection from Malicious Software

The organization shall use software countermeasures and management procedures to protect itself against the treat of malicious software. All staff shall be expected to co-operate fully with this policy. Users shall not install software on the organization's property without permission from department heads. Users breaching this requirement may be subject to disciplinary action. More details on this topic can be found in the "*Malicious Software Management*" policy.

5.13. User media

Removable electronic media of all types require the approval of department heads before they may be used on Interoptex's systems. Such media must be scanned for malware before being used on the organization's equipment. Additional details on Interoptex's policies regarding removable media can be found in Interoptex's Device and Media Control Plan documentation.

5.14. BYOD

Users are not permitted to place their personal devices (phones, tablets, personal laptops, etc.) on company networks. Interoptex will routinely review network connected devices and ban any non-approved devices of this nature. Users may access email through their phones, but must accept a policy that dictates encryption, password complexity, automatic screen lock, and a data wipe after too many failed authentication attempts. Owners of these devices are

responsible for the security and backup of these devices. (HITRUST 11190.01t1Organizational.3, 1699.09l1Organizational.10, 1326.02e1Organizational.4, 0425.01x1System.13)

5.15. Monitoring System Access and Use

An audit trail of system access and data use by staff shall be maintained and reviewed on an as-needed basis. Maintaining these systems are the responsibility of Interoptex's Engineering lead.

5.16. Accreditation of Information Systems

Interoptex shall ensure that all new information systems, applications and networks include a security plan and are approved by the Engineering lead before they commence operation.

5.17. System Change Control

Changes to information systems, applications or networks shall be reviewed and approved by the Engineering lead or Systems Administrator.

5.18. Intellectual Property Rights

The organization shall ensure that all information products are properly licensed and approved by the Engineering lead Systems Administrator. Users shall not install software on the organization's property without permission from department heads. Installing additional software is only required if the software is required to perform assigned duties. Users breaching this requirement may be subject to disciplinary action.

5.19. Business Continuity and Disaster Recovery Plans

Interoptex shall ensure that business impact assessment, business continuity and disaster recovery plans are produced for all mission critical information, applications, systems and networks. The Engineering lead, CFO, and CEO and other invested parties will meet annually to review these plans. See the "*Business Continuity Plan*" and "*Disaster Recovery Plan*" documents for additional details.

5.20. Reporting

The Engineering lead shall keep the CFO and CEO informed of the information security status of the organization by means of regular reports and presentations.

5.21. Policy Audit

This policy shall be subject to audit by the CFO and CEO. All policies and procedures will be reviewed annually and have updates applied based on lessons learned for each individual policy. (HITRUST 1667.12d1Organizational.4)

5.22. HIPAA Third Party Review

Interoptex and its business affiliates will submit to HIPAA review annually by a third party. It is the responsibility of the Security Officer to maintain the schedule for these reviews and ensure that any items defined as requiring remediation are addressed promptly thereafter.
(HITRUST 1442.09f2System.456) (0179.05h1Organizational.4)

Web Application Protection
Interoptex and its business affiliates will protect all internally developed web applications using application-level firewalling, such as AWS security groups on servers hosting web applications. (HITRUST 0808.10b2System.3)

5.23. Software Penetration Testing
Interoptex and its business affiliates will submit all software solutions developed and sold in house to annual penetration test review. It is the responsibility of the Security Officer to maintain the schedule for these tests and ensure that any items defined as requiring remediation are addressed promptly thereafter.
(HITRUST 0177.05h1Organizational.12) (HITRUST 0707.10b2System.1)

5.24. HIPAA Reminder Policy
HIPAA and security awareness reminders will be posted in all employee breakrooms and emailed to employees on a quarterly basis by the company security officer.

5.25. Network Penetration Testing
Interoptex will submit to annual third party network penetration testing. It is the responsibility of the Security Officer to maintain the schedule for these tests and ensure that any items defined as requiring remediation are addressed promptly thereafter.
(HITRUST 1413.09f2System.3) (HITRUST 0707.10b2System.1)

5.26. Budgeting
Capital planning, annual company budgeting, and investment requests will include an appropriate security resource to detail expense items required by this and other security policies to ensure resources are available for expenditure as planned. (HITRUST 0120.05a1Organizational.4)

5.27. Additional Information
Additional information and advice on this policy can be obtained from the document owner, detailed on page 1.

Company Security Officer Contact Details:
Name: Seth Hobgood
Email: shobgood@interotpex.com

Cell Phone: 615.275.5012
Desk Phone: 615.600.0090

Policy Approver:

Signature:

Name (print): Seth Hobgood

Title: CTO

Date: 02/14/18

Signature Page Follows

Corporate Information and Security Policy Acknowledgement

I, _____, have read, understand, and agree to my information security responsibilities as defined by the Interoptex Corporate Information Security Policy agreement.

Signed: _____ Date: _____