DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security – Program Requirements
PAGE: 1 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 12/31/04, 4/30/05, 1/1/09, 1/15/10, 5/1/11, 12/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.001 (formerly IS.SEC.001)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities, Company business units and all Corporate Departments

PURPOSE: To establish general, high-level requirements for the Company and Facility Information Security Programs. Information Security Standards, published on Atlas, support these high-level requirements.

Background:

Information Security strives to maintain the confidentiality, availability and integrity of Company systems and data. The Company Information Security Program helps protect the Company from incidents involving malicious software, breaches or loss of Company data, delays in patient care due to system failure, penalties due to lack of compliance with regulatory or contractual obligations (*e.g.*, HIPAA, Sarbanes-Oxley, Payment Card Industry standard), and more.

Information Protection and Security maintains documented requirements, which outline procedures and technical controls needed to effectively protect the Company's systems and data. This policy codifies those procedures and controls at a high level.

The organization of the policy statements below is based on an industry standard framework (ISO 27002). This framework is common within the information security industry to develop a comprehensive information security program. One or more Information Security Standard(s) supports each policy statement below. The standards provide more details about each of the policy statements.

POLICY:

1. Organization of Information Security – Mobile Devices and Teleworking (OIS.MDT): Company data must be protected while being processed or stored or from unauthorized access during mobile computing or teleworking.

2. Workforce Security – Secure Workforce Behavior (WS.SWB): Workforce members must receive training about information security requirements, and sanctions for violations of information security requirements.

3. Workforce Security – Termination and Change of Employment (WS.TCE): Procedures must be implemented to prevent terminated workforce members from accessing Company systems and data.

4. Asset Management – Responsibility for Assets (AM.RA): An inventory of systems and applications must be maintained to identify the Company's assets and define appropriate protection responsibilities.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security – Program Requirements
PAGE: 2 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 12/31/04, 4/30/05, 1/1/09, 1/15/10, 5/1/11, 12/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.001 (formerly IS.SEC.001)
APPROVED BY: Ethics and Compliance Policy Committee	

5. Asset Management – Information Classification (AM.IC): Electronic data must be classified according to the criteria defined in the Information Security Standards.

6. Asset Management – Media Handling (AM.MH): Handling, reuse, and sanitization procedures to protect Internal, Sensitive, and Restricted Data stored on electronic media must be implemented.

7. Access Controls – User Access Management (AC.UAM): Procedures must be implemented to ensure that workforce members have appropriate access to Company systems and data.

8. Access Controls – User Responsibilities (AC.UR): Passwords must be protected from disclosure in order to guard against unauthorized access to Company systems.

9. Access Controls – System and Application Access Control (AC.SAC): Operating systems and applications must be configured to provide secure login and authorization mechanisms in order to authenticate user identity and validate access for appropriateness before permitting access to systems that store, process, or transmit Sensitive or Restricted Data. Access to information and applications must be restricted to authorized users.

10. Cryptography – Cryptographic Controls (CG.CC): Cryptographic key management procedures must be followed and strong cryptographic keys must be used.

11. Physical and Environmental Security – Secure Areas (PES.SA): Physical security controls must be implemented to support physical security domain classifications, and those physical security controls must be regularly maintained.

12. Physical and Environmental Security – Equipment Security (PES.ES): Electronic equipment that stores, processes, or transmits Company data, must be protected from physical and environmental threats.

13. Operations Security – Operational Procedures and Responsibilities (OP.OPR): Operational procedures must be documented to support compliance with information security requirements, and to protect production systems and data from unauthorized access.

14. Operations Security – Protection from Malware (OP.PM): Company systems must be protected from malicious software.

15. Operations Security – Backup (OP.BU): Routine back up and data restoration procedures for Company systems must be documented and implemented.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security – Program Requirements
PAGE: 3 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 12/31/04, 4/30/05, 1/1/09, 1/15/10, 5/1/11, 12/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.001 (formerly IS.SEC.001)
APPROVED BY: Ethics and Compliance Policy Committee	

16. Operations Security – Logging and Monitoring (OP.LM): Systems and applications must capture system information that may be relevant to security incidents and procedures must be in place to retain this information for review in the event of a potential or actual security incident.

17. Operations Security – Technical Vulnerability Management (OP.TVM): Company systems must be protected from technical vulnerabilities through patch management or other approved mitigating controls.

18. Operations Security – Information Systems Audit (OP.A): Processes must be in place to safeguard the confidentiality, integrity, and availability of Company systems and data during information system audits or security tests.

19. Communications Security – Network Security Management (COM.NSM): Network client and infrastructure device services must be configured to reduce the ability of malicious software or users to access the Company network.

20. Communications Security – Information Transfer (COM.IT): Sensitive Data which is sent through electronic transmissions must be secured.

21. System Acquisition, Development, and Maintenance – Test Data (ADM.TD.01): Operational data must be protected from unauthorized access and modification in development and test environments.

22. Information Security Incident Management – Management of Information Security Incidents and Improvements (IM.MISI): Information security incidents must be reported; local information security incident response plans must be implemented, and must follow established Company procedures for incidents which could have an enterprise impact.

23. Information Security Aspects of Business Continuity Management– Business Continuity Management (BCM.ISC): IT&S disaster recovery and business continuity plans must be maintained and tested.

24. Compliance – Information Security Reviews (C.ISR): Information Security Policies and Standards must be periodically reviewed and revised in support of compliance with regulatory, contractual, industry standard, and business requirements. Processes and system configurations must be updated to support changes to Information Security Policies and Standards.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Security – Program Requirements
PAGE: 4 of 4	**REPLACES POLICY DATED:** 1/1/99, 8/15/01, 12/31/04, 4/30/05, 1/1/09, 1/15/10, 5/1/11, 12/1/14, 5/1/15
EFFECTIVE DATE: January 1, 2018	**REFERENCE NUMBER:** IP.SEC.001 (formerly IS.SEC.001)
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS:
Refer to the Information Security Common Terminology document for definitions.

PROCEDURE:

1. Information Protection and Security will maintain and publish Information Security Standards, which support the above policy statements.

2. Information Protection and Security will review the Information Protection Standards annually and revise as needed.

3. Exceptions to Information Security Standards must be made in accordance with the Information Security Risk Acceptance and Accountability Policy, IP.SEC.009.

4. Exceptions to Information Security policies must be approved by the Senior Vice President and Chief Ethics and Compliance Officer.

REFERENCES:

1. International Standard – ISO/IEC 27002:2013(E) – Code of practice for Information Security Controls
2. Information Security Common Terminology
3. Information Security Standards
4. Information Security Roles and Responsibilities Policy, IP.SEC.006
5. Information Security Risk Acceptance and Accountability Policy, IP.SEC.009