DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Protection Program – Security Committees
PAGE: 1 of 4	**REPLACES POLICY DATED:** 2/25/98 (IS.AA.002), 4/21/05, 1/15/10, 5/1/11, 12/1/13, 3/1/14, 12/1/14, 8/1/15, 9/1/20, 7/1/21
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.SEC.007 (formerly IS.SEC.007)
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated Divisions, Lines of Business and Facilities including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, home health and hospice, physician practices, Parallon and corporate departments.

PURPOSE:

To establish Security Committees that serve as a decision-making authority and consulting body to provide awareness, collaboration and oversight of operational actions to reduce and/or eliminate risks to sensitive company information, systems, networks, and colleagues through implementation of administrative, physical, and technical safeguards and programs.

POLICY:

1. The Director of Information Security Assurance (DISA or designee, herein referred to as DISA), must establish a Facility Security Committee (FSC) at each Company-affiliated Facility, excluding corporate, ambulatory surgery centers, home health and hospice, physician practices, Sarah Cannon research facilities, and other freestanding outpatient or learning centers (e.g., nursing schools). The DISA or designee must be the chair of this committee. This committee is an authority that makes operational decisions and addresses identified Facility-based information security concerns, thus must have adequate and recurring meetings to discuss information protection strategy at the facility level.

2. The DISA or designee must establish and maintain a Division Security Committee (DSC) at each Company-affiliated Division or Line of Business, including ambulatory surgery centers, home health and hospice, physician practices, and other freestanding outpatient or learning centers (e.g., nursing schools). The geographic composition (e.g., by division, by market, by proximity, etc.) of the DSC for ambulatory surgery centers, physician practices, HealthTrust, Parallon, CereCore, corporate, SCRI, and other freestanding outpatient centers is at the discretion of the DISA assigned to that Line of Business. The DISA must be the chair of this committee. This committee is an authority that makes operational decisions, addresses identified information security concerns, including concerns escalated by an FSC, thus must have adequate and recurring meetings to discuss information protection strategy at the facility and division level.

3. The Assistant Vice President (AVP) of Field Operations has the discretion to modify the membership requirements and meeting frequency of the FSCs and DSCs.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Protection Program – Security Committees
PAGE: 2 of 4	**REPLACES POLICY DATED:** 2/25/98 (IS.AA.002), 4/21/05, 1/15/10, 5/1/11, 12/1/13, 3/1/14, 12/1/14, 8/1/15, 9/1/20, 7/1/21
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.SEC.007 (formerly IS.SEC.007)
APPROVED BY: Ethics and Compliance Policy Committee	

PROCEDURES:

A. Responsibilities for Facility Security Committee (FSC):

1. The FSC must:
   a. Provide oversight to ensure the Facility is complying with the Company Information Security Policies and Procedures, Standards, Toolkits, Communications, Guidance and initiatives;
   b. Facilitate business decisions and development of Mitigating Control Plans (MCPs) associated with exceptions to Information Security Standards as outlined in the Accountability for Risks Associated with Exceptions to Information Security Standards Policy, IP.SEC.009, as necessary;
   c. Escalate security issues that affect a zone, market or division to the DSC.

2. The FSC must have a regular membership with voting rights. FSC members must attend regular FSC meetings in order to adequately address concerns and effectively make risk-based decisions that impact the Facility. The DISA or designee is responsible for facilitating the FSC meetings, but is not a voting member of the committee. The FSC membership must include the following facility decision makers representing both facility administration and ITG, except when the individual is not applicable to the facility setting:
   a. Chief Financial Officer
   b. Chief Operations Officer, Associate Administrator or Vice President of Operations
   c. Facility Privacy Officer
   d. Ethics and Compliance Officer
   e. Human Resources
   f. Physical Security Administrator (i.e., Plant Ops and/or Director of Physical Security)
   g. Facility IT Director
   h. Facility Emergency Operations Leader

3. The FSC members may make determinations about other key stakeholders or subject matter experts who may attend FSC meetings as participants as needed (e.g., Health Information Management Director (If not the FPO), Clinical Analyst). Participants do not have voting rights.

4. The FSC must meet quarterly or more frequently, if necessary, use the Company provided templates for meeting minutes, and develop procedures for recording, publishing, and retaining meeting minutes and related documentation per the Records Management Policy, EC.014.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Protection Program – Security Committees
PAGE: 3 of 4	**REPLACES POLICY DATED:** 2/25/98 (IS.AA.002), 4/21/05, 1/15/10, 5/1/11, 12/1/13, 3/1/14, 12/1/14, 8/1/15, 9/1/20, 7/1/21
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.SEC.007 (formerly IS.SEC.007)
APPROVED BY: Ethics and Compliance Policy Committee	

B. Responsibilities for Division/Line of Business Security Committee (DSC):

1. The DSC must:
   a. Provide oversight to ensure Division/Line of Business facilities are complying with Information Security Policies and Procedures, Standards, , Toolkits, Communications, Guidance and initiatives;
   b. Facilitate business decisions and development of MCPs associated with exceptions to Information Security Standards as outlined in the Accountability for Risks Associated with Exceptions to Information Security Standards Policy, IP.SEC.009 as necessary; and
   c. Ensure operational and technical security initiatives are aligned with Division business and operational goals.

2. The DSC must have regular membership with voting rights. DSC members must attend regular DSC meetings in order to adequately address concerns and effectively make risk-based decisions that impact the Division/Line of Business. The Director of Information Security Assurance (DISA) is responsible for facilitating the DSC meetings, but is not a voting member of the committee. The DSC membership must include the following Division/Line of Business decision makers representing both Division/Line of Business administration and ITG, except when the individual is not applicable to the Division/Line of Business setting:
   a. Chief Financial Officer or financially responsible designee
   b. Division Ethics & Compliance Officer (ECO)
   c. Human Resources
   d. Chief Information Officer (CIO)
   e. Chief Nursing Executive (CNE)

3. The DSC members may make determinations about other key stakeholders or subject matter experts who may attend DSC meetings as participants as needed (e.g., CMO, VP of Quality, Division Biomed, Regional HIM Director). Participants do not have voting rights.

   The DSC must meet quarterly or more frequently, if necessary, use the Company provided templates for meeting minutes, and develop procedures for recording, publishing, and retaining meeting minutes and related documentation per the Records Management Policy, EC.014. If there are no new agenda topics or critical discussions to review with the DSC membership from the previous quarter, then an email update to the members may be provided in lieu of in-person meeting; however, this can only be done once per year.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Information Protection Program – Security Committees
PAGE: 4 of 4	**REPLACES POLICY DATED:** 2/25/98 (IS.AA.002), 4/21/05, 1/15/10, 5/1/11, 12/1/13, 3/1/14, 12/1/14, 8/1/15, 9/1/20, 7/1/21
EFFECTIVE DATE: January 1, 2023	**REFERENCE NUMBER:** IP.SEC.007 (formerly IS.SEC.007)
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. Code of Conduct
2. Records Management Policy, EC.014
3. Record Retention and State Specific Record Retention Schedules
4. Information Security - Program Requirements Policy, IP.SEC.001
5. Information Security Roles and Responsibilities Policy, IP.SEC.006
6. Accountability for Risks Associated with Exceptions to Information Security Standards Policy, IP.SEC.009
7. Privacy Official Policy, IP.PRI.002