| | |
|---|---|
| **DEPARTMENT:** Information Protection | **POLICY DESCRIPTION:** Information Security Roles and Responsibilities |
| **PAGE:** 1 of 3 | **REPLACES POLICY DATED:** 6/1/04, 1/15/10, 11/1/12, 12/1/14 |
| **EFFECTIVE DATE:** February 1, 2024 | **REFERENCE NUMBER:** IP.SEC.006 (formerly IS.SEC.006) |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

**SCOPE:** All Company-affiliated business units and facilities.

**PURPOSE:** To outline Company Information Security roles and responsibilities, and establish the authority and guidance for the Company to appoint a Chief Information Security Officer, for each line of business or division to appoint a Director of Information Security Assurance or Director of Information Governance & Security (for HCA International), and for each Company-affiliated facility to appoint a Facility Information Security Official. The individuals assigned to these roles oversee compliance with Company Information Security policies and standards and the Company Information Security program.

**POLICY:**

1. The Company must appoint a Chief Information Security Officer (CISO) to develop, implement, oversee, and report on the Company Information Protection program and serve as the Responsible Executive for Information Security.

2. Each line of business or division must appoint a Director of Information Security Assurance (DISA) and the U.K. Division must appoint a Chief Information Security Officer (U.K. CISO) in coordination with the CISO to implement, oversee, and report on its compliance with the Company Information Security program and to oversee and coordinate efforts of its Facility Information Security Officials.

3. Each Company-affiliated facility must appoint a Facility Information Security Official (FISO) to implement, manage, and report on its compliance with the Company Information Protection program. A single individual may be appointed as the FISO for multiple facilities (e.g., in a geographic zone or market).

**PROCEDURE:**

**CISO:**

1. The CISO implements and oversees the Company-wide Information Protection program and serves as Responsible Executive for Information Security. The CISO reports to the Senior Vice President (SVP) and Chief Ethics and Compliance Officer, with dotted line reporting to both the Company Chief Information Officer (CIO) and the SVP for Internal Audit. The CISO is responsible for all Company Information Protection policies, standards, processes, procedures, infrastructures, operations, and reporting necessary to protect Company IT systems and ensure regulatory compliance. In addition, the CISO must oversee and assist business units and facilities with Information Security and related compliance program implementation.

2. The CISO's responsibilities include, but are not limited to:
   a. Overseeing the Company-wide Information Protection program to drive ongoing compliance with all applicable laws and other regulatory requirements;

b. Establishing and maintaining Information Protection policies, standards, procedures, and other guidance as needed to facilitate compliance by Company-affiliated facilities;
c. Collaborating with the SVP and Chief Ethics and Compliance Officer and the Chief Privacy Officer to ensure alignment of Company-wide compliance initiatives.
d. Engaging with Company leadership and other key stakeholders to champion business units taking ownership for incorporating Information Security controls into their business, clinical, and operational processes;
e. Collaborating with the Company CIO, division CIOs, and business unit CIOs to ensure DISA/U.K. CISO and FISO roles focus on establishing, monitoring, and reporting on Information Security controls across Information Technology Group (ITG); and
f. Championing Company-wide Information Security initiatives as needed to help business units and Company-affiliated facilities mitigate or correct identified risks to sensitive or restricted information.

**DISA/DIGS:**

1. DISA/U.K. CISO responsibilities include, but are not limited to, launching and overseeing the Information Security program for all Company-affiliated facilities, divisions, and lines of business through:
   a. Managing the governance structure for each in-scope entity (e.g., Facility Security Committee, Division Security Committee) to facilitate an effective, efficient, and standardized approach to align with the Information Protection program;
   b. Facilitating risk-based decisions by key decision-makers that focus on preventing (or correcting) identified business issues through implementation of reasonable administrative, physical, and/or technical controls;
   c. Validating and operationalizing facility readiness for internal and external audits of Information Security controls; and
   d. Partnering with ITG colleagues to assure ongoing maturity of IT operational security controls.

2. DISA/U.K. CISO serves as a key member of the ITG leadership team to drive implementation, monitor, and report on compliance with the Company Information Security policies, standards, and procedures.

3. DISA/U.K. CISO collaborates with Division/Facility Privacy Officials (FPOs), Ethics and Compliance Officers (ECOs), Information Governance Managers and Chief Nursing Officers (for HCA International), and other key decision-makers serving on the Division/Facility Security Committee to champion Information Protection program initiatives, including:
   a. Partnering on cross-disciplinary compliance activities;
   b. Partnering on cross-disciplinary incident investigation and reporting;
   c. Partnering to assure facilities are able to respond timely to time-sensitive notifications by internal or external auditors; and
   d. Partnering on communications and training for leadership and staff.

| | |
|---|---|
| **DEPARTMENT:** Information Protection | **POLICY DESCRIPTION:** Information Security Roles and Responsibilities |
| **PAGE:** 3 of 3 | **REPLACES POLICY DATED:** 6/1/04, 1/15/10, 11/1/12, 12/1/14 |
| **EFFECTIVE DATE:** February 1, 2024 | **REFERENCE NUMBER:** IP.SEC.006 (formerly IS.SEC.006) |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

4. DISA/U.K. CISO champions, administers, and provides interpretation of Information Security policies, standards, procedures, and toolkits to facilitate risk-based decisions by key stakeholders.

5. DISA/U.K. CISO directs and coordinates efforts of FISOs.

**FISO:**

FISO responsibilities include, but are not limited to, overseeing the operational aspects of each Company-affiliated facility's compliance with the Company Information Security program.

**REFERENCES:**

1. Health Insurance Portability and Accountability Act, Security Standards for the Protection of Electronic Protected Health Information
2. Payment Card Industry – PCI DSS – 12.5 Information Security Policy – Information Security Management
3. Information Security - Program Requirements Policy, IP.SEC.001
4. Information Security - Security Committees Policy, IP.SEC.007
5. Code of Conduct