Resmed and subsidiary security program

Resmed | brightree by Resmed | MatrixCare by Resmed | CitusHealth by Resmed | MEDIFOX DAN by Resmed

Table of contents

01

Introduction

Resmed is dedicated to proactively solving the complex challenges of information security, strengthening defenses against threats, and mitigating risks. We've built our processes and protocols from best practices to maintain confidentiality and data integrity for the business, our employees, our partners, and our patients.

Resmed information security vision

The security program's mandate is to support our strategy by protecting patients, data and other assets, intellectual property, brand, and partnerships.

Information security charter

The information security team helps maintain and continuously improve an enterprise information security program that effectively protects high-risk information, system integrity and availability, customer and patient data, and revenue.Security governance will direct security by design to be part of all Resmed products and services. The program is designed to meet our business's unique needs by supporting agility and innovation while fulfilling our contractual, regulatory, and ethical obligations.

Core beliefs

1. Security is invested in and treated as a strategic advantage
2. Patients and other stakeholder interests are at the core of all controls and security priorities
3. Trust has value, and loss of trust has a considerable cost, so we act decisively and assertively to mitigate risks through security controls

Who we protect

All stakeholders who use our systems and assets benefit from Resmed's security controls, including all our customers and partners

- Patients
- Doctors and clinicians
- Healthcare providers
- Distribution channel partners
- Resmedians
- Investors and all other Resmed stakeholders

02

Key features

People. A key part of our security program is the team of skilled internal and extended IT security professionals who help protect our digital information. These professionals work in areas such as:

- Security engineering
- Security architecture
- Cloud security architecture
- Security governance (which includes policy, standards and process)
- Security operations & monitoring
- Security risk management
- Security incident response planning
- Vulnerability management
- Regulatory compliance
- Project management (security-specific tool and process implementation)

Our security staff holds numerous certifications,which include:

- Master of Business Administration (MBA)
- Master of Science in Information Security (MSIS)
- Master's in advanced IT security and digital forensics
- Certified Information Systems Security Professional (CISSP) from International Information Systems Security Consortium (ISC)2
- Critical Incident Stress Management (CISM) and Certified in Risk and Information Systems
- Control (CRISC) from Information Systems Audit and Control Association (ISACA)
- Certified Information Privacy Professional (CIPP from International Association of Privacy Professionals (IAPP)
- ISACA certified from COBIT Foundation
- Foundation certificate (SCF) from Sherwood Applied Business Security Architecture (SABSA)
- Information Technology Infrastructure (ITIL) certified
- TOGAF 9 Certified from The Open Group
- EC-Council Certified Ethical Hacker (CEH 9)
- ISO/IEC 27001: 2005 ISMS Lead Auditor
- GIAC Certified Forensic Analyst (GCFA
- Amazon Web Services (AWS) Business Professional
- Certificate of Cloud Security Knowledge (CCSK) from Cloud Security Alliance (CSA)
- AWS Certified Developer Associate
- GIAC Certified Incident Handler (GHIC)

Process. Our processes were built to help ensure high-quality in data protection, risk assessments, and project and purchase support. These processes are supported by:

Information Security Framework

This document outlines how we assess and manage risks. It's broken into steps to identify potential threats,protect against known and unknown threats,proactively detect threats, respond appropriately, and recover any compromised data or assets.

Governance

This document outlines our policies, standards, guidelines, and processes for protecting against information security.

Technology. Our current technology uses robust tools to provide security issue transparency, anomaly detection, vulnerability management, security monitoring,access controls, and security and risk management.

In the constantly evolving landscape of information security, we'll continue building on our current technology. Looking ahead, we're increasing automation and orchestration, and enabling emerging technologies to support evolving business needs—such as cloud-based data storage, IoT, data analytics, AI, and machine learning.

Security architecture – defense in depth

Layers	Threats	Defenses
Physical	Physical intrusion, social engineering	Badged access, data center controls, training, assessments
Cloud	Data loss, misconfiguration	Data loss prevention (DLP), configuration monitor, security information and event management (SIEM), web application firewall
Network	Hacking, denial of service (DOS)	IDS/IPS firewalls, Strict ACLs virtual private network (VPN), app security, SIEM
Platform	Phishing, malware, hacking	Employee training, phishing campaigns, URL filtering, security ops center, email security
PCs and mobile	Malware, ransomware, hacking, device loss	Traditional and next-generation anti-virus, device encryption, asset management
Application	SQL injection, man-in-the-middle, software vulnerability, hacking	Penetration testing, coding standards, patching, secure software development life cycle (SDLC)
Data	Unauthorized access	Encryption, IDS/IPS firewalls, backup/recovery, VPN, Multi-factor authentication (MFA)
Response	Security event, breach, data corruption or loss, system loss	SIEM incident response, dedicated security team, third-party support

03

Security operations

Our security operations team works in conjunction with our IT teams for cohesive infrastructure, application development, project management, and systems support. Security operations include:

- Security operations center (SOC) that is open 24 hours a day, seven days per week
- Monitoring
- Ticket management
- Cloud security

Incident response

We have a well-documented and tested incident response program, which includes numerous function runbooks. Tabletop exercises are performed and continue to expand as the program matures. Incident response processes include incident triage, well-defined roles and responsibilities, a communications plan (including customer notification), formal rules on evidence management and documentation, and designated incident leadership.

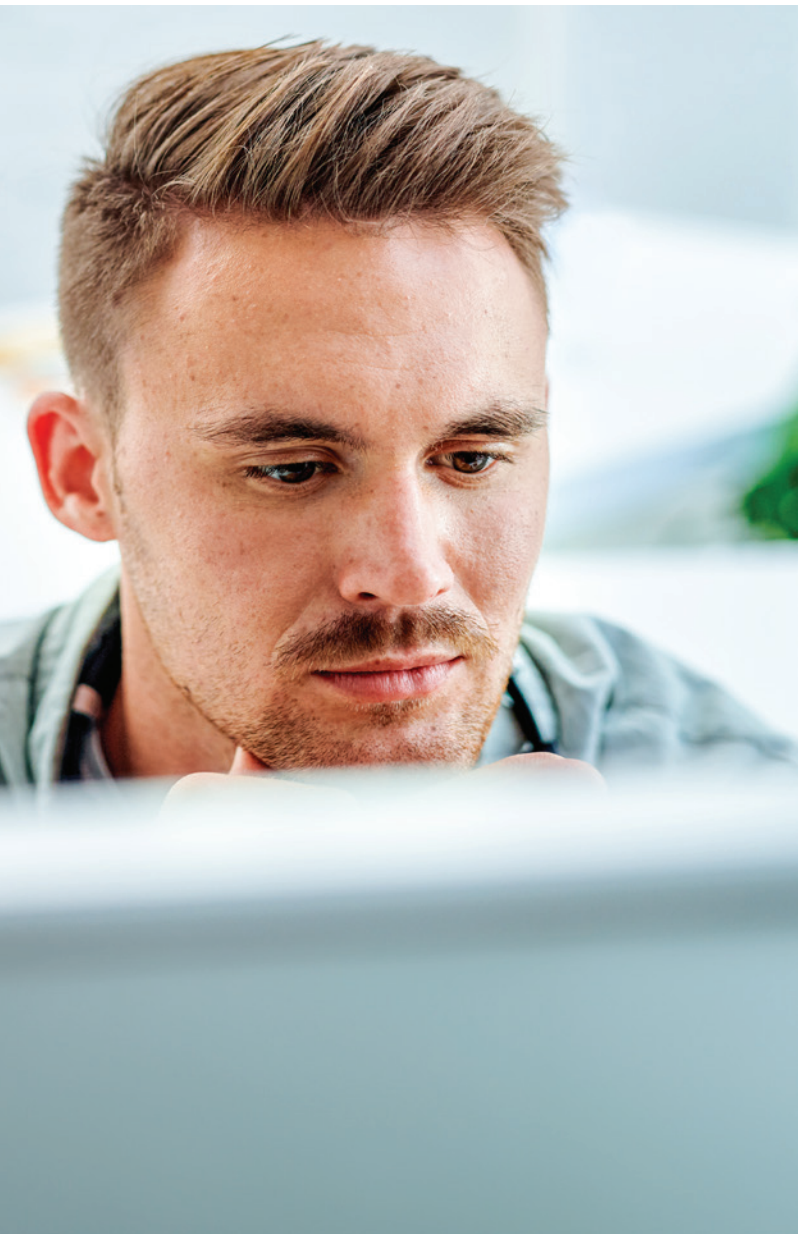
24/7

365

04

Risk and threat management

All security initiatives are prioritized based on business risk, and security risks are tracked in a formal governance risk and compliance (GRC) management tool. Security risks are reviewed to ensure risk rankings are accurate and driving the appropriate prioritization and investments. Risk management processes include:



- Risk analysis
- Risk register
- Prioritization
- Tracking

Assessing vulnerability and threat management

We leverage our pool of resources from all our companies to collect and distribute the latest threat intel in a standardized format. This allows everyone to take the same actions simultaneously to mitigate or minimize the risk of the latest threats and vulnerabilities. In addition, our global team has standardized vulnerability assessment tools to identify, monitor and report threats in our environments. Annual third-party assessments are also conducted on our key applications and infrastructure.

Vendor management and third-party risk management

All Resmed vendors or third parties that transmit, process or store sensitive data are regularly reviewed to ensure compliance with proper security and regulatory standards. Those failing to comply are required to address the gap(s) in a time period based on the severity of the risk.

Summary

To summarize, our employees, customers, patients, investors, and partners depend on the security of our information systems and technology. Our team of experts, spanning various areas of information security, works collaboratively to help ensure we proactively safeguard against threats and have the processes and protocols in place to respond quickly and help eliminate them.