ResMed and subsidiary security program

ResMed

MatrixCare by ResMed | brightree by ResMed | CitusHealth by ResMed

Distributed by ResMed Corp, 9001 Spectrum Center Boulevard, San Diego, CA 92123 USA. (858) 836-5000 or (800) 424-0737 (toll free). See ResMed.com for other ResMed locations worldwide.
Specifications and content may change without notice. For patent and other intellectual property information, see ResMed.com/ip. 10111786/1 2020-04

Table of contents

01 Introduction

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

ResMed information security vision

The ResMed security program's mandate is to support ResMed's strategy through the protection of patients, data assets and other assets, intellectual property, brand and partnerships.

Information security charter

The information security team at ResMed is in place to maintain and continually improve an enterprise information security program that effectively protects high-risk information, system integrity and availability, customer and patient data, and ResMed revenue. Security governance will direct security by design to be part of all ResMed products and services. The program will meet the unique needs of our business by supporting high velocity and innovation while satisfying our contractual, regulatory, and ethical obligations.

Core beliefs

To support the vision of the information security team, we operate under these core beliefs:

1. Security is treated and invested in 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 ResMed systems and assets are beneficiaries of ResMed security controls. These include all of our customers and partners:

- Patients
- Doctors and clinicians
- Healthcare providers
- Distribution channel partners
- ResMedians
- Investors and all other ResMed stakeholders

02
Key features

People

One of the most important components of our security program is the skilled internal and extended IT security professionals who work to ensure that our digital information is protected. 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's in business administration (MBA)
- Master's in information security (MSIS)
- Master's in advanced IT security & digital forensics
- Certified Information Systems Security Professional (CISSP) from International Information Systems Security Consortium (ISC)^2
- Critical Incident Stress Management (CISM) & 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)
- Foundation certificate (SCF) from Sherwood Applied Business Security Architecture (SABSA)
- ISACA certified from COBIT Foundation
- Information Technology Infrastructure (ITIL) certified
- TOGAF 9 Certified from The Open Group
- E-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 ensure the highest 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 policy, standards, guidelines and processes against threats to 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 to build on our current technology. Looking forward, we are working to increase automation and orchestration, and enable emerging tech to meet business needs that include: cloud-based data storage, IoT (Internet of Things), data analytics, artificial intelligence and machine learning.

The ResMed and subsidiary companies have numerous controls, including many of the following:

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 devices	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 information technology 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

ResMed has a well-documented and tested incident response program, which includes numerous function run books. Tabletop exercises are performed and are being expanded as the program matures. Incident response processes include incident triage, well-defined roles and responsibilities, communications plan (including customer notification), formal rules on evidence management and documentation, and defined incident leadership.

04 Risk and threat management

• • • •

Risk 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 upon the security of our information systems and technology. Our team of experts from a variety of areas in information security work collaboratively to ensure we proactively safeguard against threats and have the processes and protocols in place to quickly eliminate them.

ResMed

MatrixCare® by ResMed

brightree® by ResMed

CitusHealth® by ResMed

Distributed by ResMed Corp, 9001 Spectrum Center Boulevard, San Diego, CA 92123 USA. (858) 836-5000 or (800) 424-0737 (toll free). See ResMed.com for other ResMed locations worldwide.
Specifications and content may change without notice. For patent and other intellectual property information, see ResMed.com/ip. © 2020 ResMed. 10111786/1 2020-04