Palomar®

PALOMAR CYBERSECURITY STATEMENT

Palomar recognizes the importance in protecting customer's data and digital assets in our care. Thus, at Palomar we have worked diligently in creating a layered security posture leveraging people, process, and technology. This mindset is embedded throughout our operations and technical programs.

As a foundation, Palomar maintains a suite of information security, privacy, and data protection related policies, standards, and procedures leveraging the National Institute of Standards and Technology ("NIST") along with the COBIT 2019 framework to align with applicable laws, regulatory guidance, and industry acceptable best practices.

Additionally, Palomar continues to mature its threat hunting, proactively searching for and identifying malicious attacks, and testing our cybersecurity posture to further enhance our cybersecurity programs. This analysis includes comprehensive risk analysis of our assets along with routine external penetration testing from third party providers.

From a personnel perspective, we require mandatory cybersecurity, privacy, and information handling training for all team members and non-team members upon onboarding and then on an annual basis thereafter. Additional role-based training is provided to the security, IT operations, and development teams. Palomar also leverages a monthly hints and tips and weekly scam of the week campaigns to keep team member updated and aware of the current cyber threats. To validate the effectiveness of the training a simulated phishing campaign is setup to run on a monthly basis against all users.

As part of the Palomar technology perspective, we leverage a variety of tools to protect information. These tools include but are not limited to multifactor authentication, firewalls, Intrusion detection, vulnerability and penetration testing, central log management, endpoint protection and patch management systems. Our identity and access management systems include industry leading products leveraged through our best practices internally developed solutions. We also leverage cutting edge threat hunting services that actively monitor for anomalies on our network and application events which then investigate and escalate these anomalies to the Security Operations group.

Palomar also participates in the American Property Casualty Insurance Association ("APCIA") to share insurance innovation and technology and participating in cyber security vulnerabilities along with engaging in state and federal regulatory discussions

Finally, Palomar has a Security Incident Response Framework ("SIRF"), a Disaster Recovery ("DR") and Business continuity ("BCP") plans in place. The SIRF is a set of procedure and tasks that outline the steps the incident response team executes in the event of a cybersecurity incident. These procedures and task are designed to ensure the event timeline is accurately documented and the resolution is done in a timely manner. The DR plan is comprised of a variety of policies and procedures around our vital services to ensure service disruption is minimal in the event of a disaster or human induced incident. Our BCP strategy is similarly developed around policies, procedures and tools to minimize the financial impact to Palomar and continue to serve our customers.

These three frameworks are tested annually through a tabletop process involving the business and IT operations staff to ensure the plans are still covering all relevant and critical services and ensures the stakeholders are prepared.

Palomar's Board of Directors are regularly briefed by Management on cybersecurity matters that would include threats, policies, practices, and the roadmap being implemented to improve the security posture. Ongoing cybersecurity improvements may include the results from the tabletop exercises, Enterprise Risk assessments, penetration testing to provide internal assessments along with independent third parties around Palomar's technical program and the ability to respond to an incident.

Combining all these items into a single, integrated framework, an overlapping strategy based upon people, technology and processes will yield the most effective defense. Creating a strong culture of security within Palomar along with conducting threat research, prioritizing our assets, and deploying security controls within our applications will enhance visibility and shorten threat response times. The results of this effort will minimize the impact of any cyberattacks.