# Our Commitment to Protecting Your Data

Newport understands how important information and data security is to your business and ours. The trust you place in us to protect your important and often confidential information forms the foundation of our long-term relationship, and we understand our obligations to manage it effectively and securely.

We continually monitor and address cybersecurity risks, invest in state-of-the-art technology, and enhance our information security best practices.

Because of our continued focus on safeguarding data, **Newport is in alignment with best practices for recordkeepers and providers as outlined by the Department of Labor**.

These best practices identified **12 areas of focus for recordkeepers and providers—and Newport's cybersecurity program meets or exceeds each of the best practice recommendations**. The following is an overview of these 12 areas, along with details of how Newport is continually expanding, enhancing and evolving our cybersecurity capabilities, practices and protections.

This is part of our ongoing commitment to stay ahead of new and emerging threats in an ever-changing cyber risk landscape—and help keep your important information safe.


## A FORMAL, WELL DOCUMENTED CYBERSECURITY PROGRAM

Newport maintains a formal, documented **IT Security and Governance Policy** that requires the documentation, implementation, enterprise-wide adoption and continuous operational compliance with all information security policies, procedures, guidelines, and standards, to protect the security of the technology infrastructure and data stored on our systems, and those of our providers and partners.

Newport security policies are reviewed at least annually and updated as needed by the Chief Information Security Officer, formally approved for adoption by the Enterprise Risk Management Committee and distributed to all employees upon hire and major modification.

Newport's IT security program undergoes multiple external assessments and reviews annually by independent third party auditors, to include SOC 1 and SOC 2 audits, producing an annual Report on Controls for each.

Copies of Newport's current IT Security and Governance Policy and SOC reports are available to clients upon request.

 


## PRUDENT ANNUAL RISK ASSESSMENTS

Newport performs comprehensive risk assessments at least annually. Identified risks or threats are evaluated, prioritized, treated and documented.


## A RELIABLE ANNUAL THIRD PARTY AUDIT OF SECURITY CONTROLS

Newport undergoes multiple external assessments and reviews annually by independent third party auditors, to include SOC 1 and SOC 2 audits, and annual penetration testing. Any cybersecurity risks or threats identified through such third party audits are evaluated, prioritized, treated and documented.

Copies of Newport's SOC reports are available to clients upon request.


## CLEARLY DEFINED AND ASSIGNED INFORMATION SECURITY ROLES AND RESPONSIBILITIES

Information Security Roles and Responsibilities are defined and documented in Newport's IT Security and Governance Policy. Newport's Cybersecurity Team is part of our Technology and Digital Innovation group, which is comprised of experienced and qualified information technology and cybersecurity experts. The Chief Information Security Officer (CISO) establishes and maintains the vision, strategy, and operation of the cybersecurity program, which is performed and maintained by qualified personnel. Collectively, the Newport Cybersecurity Team holds more than 15 industry recognized cybersecurity, privacy and risk management certifications and accreditations.


## STRONG ACCESS CONTROL PROCEDURES

Newport's IT Security and Governance Policy provides for strong identity and access control, requiring that the "principle of least privilege" be uniformly applied, along with the use of role-based access control, to ensure that access to sensitive and privileged information remains appropriately restricted to only those with authorization and a valid business need. Newport employs a layered, defense-in-depth access controls strategy across the enterprise, including scenario-driven combinations of the following:

- Unique and complex passwords and passphrases and multifactor authentication methods
- Location and context-based conditional access decision engines
- Hardware-based identity proofs
- Step-up controls for elevated access permissions and privileged functions

To ensure that permissions remain accurate and always up-to-date, Newport performs quarterly entitlement reviews of all individual and group access and authorization permissions. User access privileges are promptly revoked for employees terminating their employment with Newport.


## ASSETS OR DATA STORED IN A CLOUD OR MANAGED BY A THIRD PARTY SERVICE PROVIDER ARE SUBJECT TO APPROPRIATE SECURITY REVIEWS AND INDEPENDENT SECURITY ASSESSMENTS

Newport requires vendor due diligence, including a comprehensive cybersecurity review before any Cloud, or other external service provider, may be used for storage of any assets or data. All such vendors and uses are reviewed at least annually and reauthorized for use. Annual reviews include establishing annual recertification criteria, such as ongoing risk assessments, requiring that external service providers perform annual SOC audits and/or maintain industry certifications, as applicable. Newport's service agreements with such vendors require that Newport be notified immediately of any cybersecurity event which directly impacts a customer's information system(s) or nonpublic information.


## CYBERSECURITY AWARENESS TRAINING CONDUCTED AT LEAST ANNUALLY FOR ALL PERSONNEL AND UPDATED TO REFLECT RISKS IDENTIFIED BY THE MOST RECENT RISK ASSESSMENT

All persons having access to Newport systems or data must complete mandatory cybersecurity awareness training at time of hire, and then at least annually thereafter. Periodic reminders and security updates are distributed to employees throughout the year to help maintain heightened awareness of cybersecurity risks. Additionally, we perform ongoing testing of cybersecurity readiness, to ensure appropriate responses to risk scenarios, such as phishing or fraud attempts, and individuals working in certain specialized job functions are required to complete role-specific training at least annually.


## SECURE SYSTEM DEVELOPMENT LIFE CYCLE PROGRAM (SDLC)

Newport employs a "secure by design, secure in development, secure in deployment and secure by 'default' strategy." This includes the use of robust Static Application Security Testing and Dynamic Application Security Testing tools and techniques. We perform continuous scanning across all systems as a part of our enterprise-wide vulnerability management program, as well as penetration testing of all external and customer-facing applications.


## A BUSINESS RESILIENCY PROGRAM WHICH EFFECTIVELY ADDRESSES BUSINESS CONTINUITY, DISASTER RECOVER, AND INCIDENT RESPONSE

Newport maintains detailed Disaster Recovery (DR) and Business Continuity Plans (BCP) which are tailored for each area of Newport's business, and designed to ensure the continuity of business operations in the event of disaster or disruption. Additionally, our Cybersecurity Incident Response and Crisis Management Plans provide that appropriate staff are properly trained and ready to act quickly if a cybersecurity incident or other crisis occurs, to safeguard people, data and systems assets, while minimizing business disruptions to the fullest extent reasonably possible.

All plans are reviewed and updated at least annually, and regularly tested to ensure appropriateness, readiness, and effectiveness.

## ENCRYPTION OF SENSITIVE DATA STORED AND IN TRANSIT

Newport uses and supports the most current data encryption standards available to protect the confidentiality and integrity of sensitive data and non-public information when stored at rest and during transmission in transit.

## STRONG TECHNICAL CONTROLS IMPLEMENTING BEST SECURITY PRACTICES

Newport utilizes industry recognized security tools, technologies and solution eco-systems. Technical security solutions contained in the hardware, software, or firmware components of Newport's system include:

- Consistent model and version updates
- Vendor-supported firewalls, intrusion detection and prevention appliances/tools
- Routine patch management
- Automated data backup

## RESPONSIVENESS TO CYBERSECURITY INCIDENTS OR BREACHES

Newport's Incident Response Plan provides guidance for immediate and appropriate investigation and remediation in case of an incident. These protocols are in place to mitigate any harm caused and prevent recurrence. Our plan requires impacted party notification based on the circumstances, which may include, as applicable, the impacted plans and participants, law enforcement, Newport's insurance carriers, and other parties required pursuant to applicable law.

## FOR MORE INFORMATION

Additional information about Newport's IT and Cybersecurity Programs is available to clients upon request. Contact your Newport relationship manager for details.



1350 TREAT BOULEVARD, SUITE 300, WALNUT CREEK, CA 94597

VISIT **NEWPORTGROUP.COM**