



Security at Ampion

Ampion operates at the intersection of energy and information technology, two domains that are highly regulated and complex with respect to legal protections of mass-market consumers and commercial off-takers. The repercussions of a security or compliance breach can be severe and expensive. Therefore information security, privacy and regulatory compliance are central to our solution.



Nacha



DataGuard
Energy Data Privacy Program

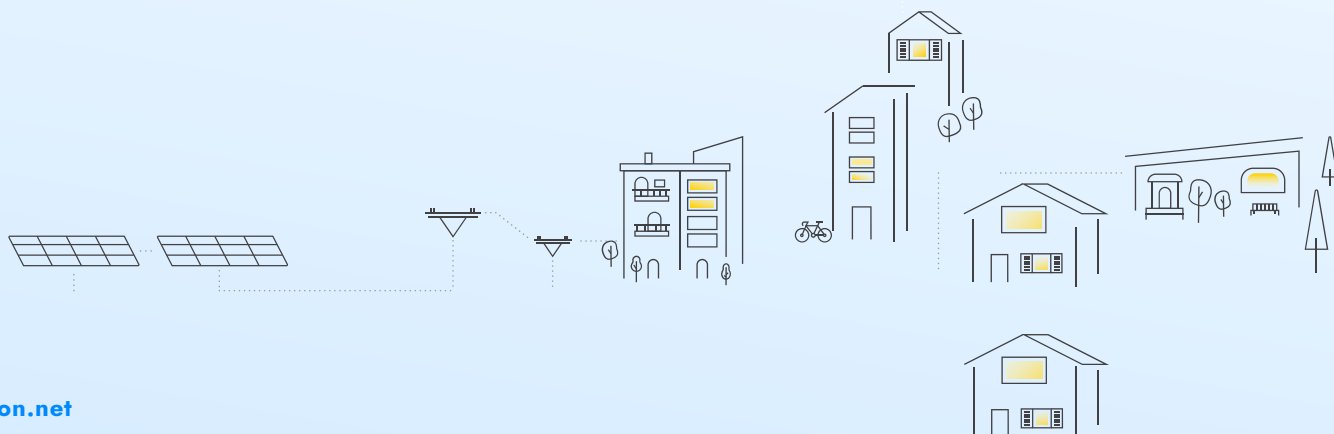


Security Standards Council

SECURITY AT AMPION

Compliance

Failure to comply with applicable laws governing community solar programs, consumer marketing of energy, and online payment processing can literally stop an operator in their tracks. The financial and reputational risks are substantial and our clients rely upon us to eliminate their exposure. As such, Ampion's dedicated policy team ensures we comply with the strictest of state, federal, and international regulatory standards such as PCI, Nacha, HEFPA, MA 201 CMR 17, CCPA, UBP-DERS, FCRA, FTC Red Flags Rule, DataGuard and others.





SECURITY AT AMPION

End-point and Cloud Systems Security

Cybersecurity is paramount when managing personally identifying data and associated payment credentials. Ampion conforms to the vital standards of end-point and cloud system security protecting against data breaches and loss of confidentiality. We consider vulnerabilities at 8 OSI layers, administering robust protections wherever applicable.



SECURITY AT AMPION

Risk Management

Ampion's ISO27001 Certification is the foundation for our exhaustive and continuous effort to identify and control business and security risks through rigorous preventative maintenance measures, and aggressive incident response. The continual nature of the engagement and regular external oversight ensures that Ampion remains at a high level of security and preparedness.



SECURITY AT AMPION

Social Engineering Threat Mitigation

Even the best protected platforms may be vulnerable to malicious attacks that leverage gaps in the training and behavior of personnel. Ampion implements numerous measures to address social engineering campaigns, and uses a highly agile and adaptive curriculum to ensure our employees are thoroughly vetted and constantly well educated to identify and remediate emerging cybersecurity threats.

