Privacy and Security
Leading the industry with SOC 2

Table of Contents

Introduction ................................................................. 2
What is the Value of SOC2? .................................................. 3
Building on a Foundation of Privacy and Security .................. 3
Facilities ........................................................................ 3
Secure Framework ........................................................ 4
Secure Data Transfer and Storage ...................................... 4
Secure Web Infrastructure ................................................ 4
System and Network Monitoring ......................................... 4
Personnel ....................................................................... 4
Introduction

Utilities around the world are recognizing the importance of engaging their customers with data-driven insights about their energy use. This is a critical need in regions undergoing a smart grid rollout where energy insights based on smart meter data can be the most tangible aspect of value for customers.

Utilities face a dilemma in addressing this need. How can they ensure customer privacy, data security and meet regulatory requirements while also partnering with advanced providers of analytics and multi-channel engagement?

To address this dilemma, over 80 utilities around the world have partnered with Opower. Each of these partnerships represents a utility’s trust in our ability to protect its customer information. This further reflects Opower’s commitment to invest as aggressively in cutting-edge security infrastructure and privacy practices as we do in behavioral science, big data analytics and UX design. We have earned this trust with our best in class information security and privacy standards, which have been approved by internationally recognized third party auditors and the largest American utilities.

While data privacy and security expectations vary by country, Opower consistently works to ensure that our information security framework meets and exceeds applicable legal and regulatory bars, including compliance with the European Union Directive on Data Protection and obtaining certification under the EU-US Safe Harbor Framework. To further objectively verify these investments and practices, Opower ensures transparency and operational assurances by working with industry leading auditors to bring additional levels of audited scrutiny to the security and privacy of our platform and business processes. Effective January 2013, Opower is proud to announce that we have now achieved the gold standard in third-party verified information security assurances—known as SOC 2 Type 2. Awarded by Deloitte & Touche, Opower’s SOC 2 certification firmly establishes it as the market vanguard for protecting customer data. This certification builds on a foundation of privacy and security investments and further establishes Opower’s track record of industry leadership.

In addition to earning the trust of utility partners, we are committed to helping these utilities earn the trust of the 15 million utility customers that they serve around the world. We do this by offering a TRUSTe certified privacy policy, certification that Opower adheres to the US-EU Safe Harbor Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information from European Union member countries, and a set of Data Privacy Principles that simply communicate how we intend to use customer data across our service offerings in ways to enhance value while protecting privacy.
What is the Value of SOC2?

SOC 2 is an examination, conducted by Deloitte & Touche LLP, that provides transparency and market credibility through intensive independent auditing of controls related to the Opower 4 Customer Engagement Platform. The SOC 2 Type 2 report indicates that controls were suitably designed and operating effectively over a period of time to meet the criteria for representing the security and confidentiality principles set forth in Trust Service Principles (TSP jointly set by the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

As part of this exhaustive audit, SOC 2 requires Opower to design, document, and incorporate an information security strategy that comprehensively adheres to AICPA’s Trust Services Principles. In aligning ourselves with this standard, we are building on our use of the existing Smart Grid industry standards put forth by the National Institute of Technologies (NIST) under Guidelines for Smart Grid Cyber Security (NISTIR 7628), and going further by adopting a range of best practices based on emerging domestic and global data privacy requirements. Moreover, our attainment of the SOC 2 Type 2 standard provides ongoing, objective third-party audits and verification on an annual basis that strengthens and leaves no ambiguity about our company’s commitment to information security and data protection of our services.

Building on a Foundation of Privacy and Security

While SOC 2 represents a significant investment on behalf of our clients in bringing additional levels of scrutiny, Opower has made a series of key investments in privacy and security in years prior to this certification.

In early 2012, we published a set of Data Privacy Principles to help customers understand how Opower provides insight, transparency in how we use and protect their privacy and puts them in control. In June, Opower implemented an all-encompassing approach to data privacy and security consistent with each of the seven foundational principles of Privacy by Design. Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

The following section details a few examples of the many investments we have made across facilities, data transfer, web infrastructure, system and network monitoring and personnel in order to achieve these certifications.

Facilities

Opower uses enterprise grade datacenters that are SSAE-16 SOC I and Tier III certified. Among other measures, these facilities offer industry leading digital video security surveillance, 24x7 on site security personnel and redundant power, network and cooling capabilities. Physical access to machines is restricted to authorized personnel with biometric access controls. These controls ensure the data remains physically secure within Opower’s infrastructure.
Security Framework
Opower uses a defense in-depth strategy to ensure the security of utility customer data based upon nationally recognized Smart Grid cybersecurity standards. The Opower network and applications are built upon multiple layers of defenses, including but not limited to firewalls, intrusion detection and prevention capabilities, role-based access controls and 24x7 monitoring. Additional protections built into the platform are designed to protect against potential attacks and breaches.

Secure Data Transfer and Storage
As part of Opower’s Data Transfer Standards, all utility data transferred to and from Opower is encrypted for security and confidentiality purposes. Utilities transfer data to Opower using the Secure File Transfer Protocol (SFTP) with 2048-bit key-based encryption technologies, a level of encryption that is used in online banking transactions. Once data is in the Opower platform, Opower has the capability to deploy data encryption technologies to further enhance the security measures around personally identifiable. Opower uses a tiered infrastructure platform to provide high availability, reliability and data protection. Opower provides disaster recovery capabilities in geographical disparate locations ensuring service resiliency across the platform. Additionally, Opower encrypts backups using the AES encryption algorithm to ensure backup data is appropriately protected.

Secure Web Infrastructure
All communications from Opower to customers and utility personnel (via the Customer Service Representative portal) are also encrypted in transit via SSL with 128-bit encryption. Opower’s website utilizes HTTPS for securing web server to client communications. This establishes the encryption of the session, ensuring the confidentiality, integrity and authenticity of data transmitted between the end-user and the application.

System and Network Monitoring
Opower’s systems and network are monitored for security incidents, network intrusions, vulnerabilities, system health and availability. In the event of a security breach, the Opower Incident Response team, comprised of stakeholders from key departments, performs a risk-based assessment of the situation and develops appropriate mitigation strategies, while working with utility security counterparts.

Personnel
Opower has a dedicated experienced internal information security team that focuses on operational risks consistent with the privacy policy, data principles and data protection controls within the infrastructure are being implemented and operating as designed. Opower restricts access to client data to authorized employees who require access to configure, administer or deliver Opower services based on a least privilege model. Opower’s employees and vendors are bound by strict confidentiality terms, acceptable use and corporate policies. Each Opower employee undergoes mandatory security awareness training, regardless of his or her role.