Info Sheet

A Focus on Security and Compliance

Security is woven throughout Optimal IdM operations and approach

A defined security program that controls everything from pre-employment background checks to the development environment to cloud service operations is the bedrock of what we do.

Highlights

- Compliance Measures
- Development Security
- Production Environmenets
- Employment Practices

Compliance Measures

Optimal IdM undergoes an AICPA SOC 2 Type II audit each year to verify compliance to its security program, policies and procedures, and industry standards. Optimal IdM also complies with the EU Standard Contractual Clauses for the protection of personal data of EU citizens. These model clauses are in place for several of our European clients and we have implemented these requirements with our vendors; such as Microsoft. Optimal IdM is on schedule for full compliance to the EU General Data Protection Requirements (GDPR) for its deadline of May 2018.

Development Security

All code is maintained for safekeeping in a secure software vault. Developers check out the code to make design modifications which have been approved in advance. The developers operate in isolated virtual environments to make the changes and test the revised code. All code is tested for the Open Web Application Security Project (OWASP) Top 10 Security Risks and Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors. This testing checks for vulnerabilities such as buffer overflow, cross-site scripting and command injection to assure a robust and secured product is released.

Production Environments

For years Optimal IdM's flagship product, VIS or Visual Identity Server, operated as a local install in client datacenters. With the rise in popularity of cloud based systems in recent years, Optimal IdM released a cloud solution based upon their proven product. This cloud solution uses the expertise and strength of Microsoft to run in Microsoft datacenters in Azure environments. These state-of-the-art datacenters are located around the globe and are used by numerous international corporations. Our preferred deployment model is redundant dedicated servers in multiple datacenters with separate environments for test and production.

Microsoft is responsible for all infrastructure management such as physical access security, power and connectivity, replication to hot sites, and network security. All communications to these servers is through secured, encrypted channels. Annual audits certify Microsoft operates these datacenters in accordance with their security program and industry standards. This leaves Optimal IdM to focus on its core competency of identity management.

Only authorized Optimal IdM system administrators have access to the customer server environments and multi-factor authorization is used to confirm their identity at login. In addition to being backed up on a frequent basis, the servers are continuously monitored for unusual or suspicious behavior.

Employment Practices

All employees and contractors undergo a thorough pre-employment background check before access to company information is granted. Confidentiality and non-disclosure agreements protect both company and client information from unauthorized disclosure. Personnel receive training on security and key aspects of their job. User access is granted on as needed basis at the lowest level required to company and client systems. All of these processes are defined in an employee handbook and company policies which are reviewed and distributed each year.

Many of our employees attend industry conferences each year and are featured as expert speakers on a variety of identity management topics. This knowledge is passed through our company via training sessions and weekly technical meetings.