Security Overview

Methodology

At Employee Navigator, we achieve the highest level of security by performing full security audits of our product and infrastructure regularly. Our security practices have been evaluated as part of our SOC 2 Type I attestation.

Encryption Security Overview

Your transmitted data is kept safe using the highest encryption standards available, including 256-bit SSL encryption. This is the same technology that banks use to keep your account information safe and all account information you provide, including passwords and personal information details, is protected using this technology.

Backup

Employee Navigator employs state of the art back-up and firewall technology to ensure that your information is always available, no matter what happens. Our system stores back-ups in multiple secure locations and is updated throughout the day, every day.

Physical Security

Our servers are hosted at Tier III, SSAE-16 and ISO 27001:2005 compliant facilities which are Safe Harbor Certified. Our facilities feature 24-hour manned security, biometric access control, video surveillance, and physical locks. The co-location facilities are powered by redundant power, each with UPS and backup generators. All systems, networked devices, and circuits are monitored by both Employee Navigator and the co-location providers.

Secure at Every Step

We built the Employee Navigator product entirely on our own so we are able to monitor and keep safe every aspect of our software. All access to data within Employee Navigator is governed by access rights, authenticated by username and password and your Employee Navigator instance administrator can define granular access privileges. Employee Navigator also follows secure credential storage best practices by storing passwords using the bcrypt (salted) hash function. Our security architecture ensures segregation of customer data and stricter access restrictions for Employee Navigator's HR mobile app.

Behind the Scenes

Employee Navigator's multi-pronged approach to security ensures you are protected at all times. We adhere to industry standards for protecting your data, securing our web application, and processing all transactions. We've created policies across our entire organization to ensure that Employee Navigator offers the highest level of security.

SOC 2

Employee Navigator has completed the SOC 2 Type 1 Audit. A SOC 2 report is intended to evaluate an organizations information systems relevant to security, availability, processing integrity, confidentiality & privacy. Employee Navigator's SOC 2 report is available upon request.

HIPAA

There are no official government or industry certifications for HIPAA compliance. In order to support HIPAA compliance, Employee Navigator has reviewed the HIPAA regulation and updated its product, policies and procedures to support customers around their need to be HIPAA compliant. The Employee Navigator product/platform meets the obligations required by HIPAA, however customers are also responsible for enforcing policies within their organizations to meet HIPAA compliance. Some of Employee Navigator's controls that are relevant to HIPAA include:

- Controls to provide reasonable assurance for defining and granting access to users permitted by the users entity.
- Controls to provide reasonable assurance that the user entity's method for accessing Employee Navigator application is configured with proper logical security protocols.
- Controls to provide reasonable assurance that user accounts and access permissions are correctly specified on an ongoing basis, including revoking accounts.