EQUIFAX®

# The Work Number

## Best Practices in Data Management

Leadership in security is fundamental to our basic purpose—empowering businesses and consumers with information they can trust. Equifax Workforce Solutions treats its security practices with utmost importance. This allows us to thoughtfully and effectively manage the evolving threat landscape and dynamic compliance requirements.

The Equifax Global Security mission statement expresses the totality of this commitment: to provide global assessment, design, development, delivery, and monitoring of the security assets of Equifax.

It is important to make sure that any partner you consider that will handle your employees' personal information has top-notch security. Below is a short list of some of these steps we take to keep our clients' data secure.

| CERTIFICATION / INDUSTRY BEST PRACTICE(S) | DESCRIPTION |
|---|---|
| **SOC 2 Type II** | Service Organization Control (SOC) 2 Reporting on controls at a Service Organization relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy as published by the American Institute of Certified Public Accountants' (AICPA) |
| **FISMA ATO - NIST Moderate** | Information security standards defined by the Federal Information Security Management Act and administered by National Institute of Standards and Technology (an agency of the US Department of Commerce). Demonstrates a foundational level of security suitable for data exchange with critical government systems. Assessments occur on a continuous monitoring schedule to maintain the Authority to Operate (ATO). |
| **ISO/IEC 27001:2013** | A set of security standards administered by the Internal Organization for Standardization (ISO), which specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization. Equifax is ISO/IEC 27001:2013 certified by a reputable independent third party. |

| CERTIFICATION / INDUSTRY BEST PRACTICE(S) | DESCRIPTION |
|---|---|
| **Risk Based Authentication** | Takes into account several attributes of the end user requesting access to the system to determine the risk level and may apply a challenge/ response process with complexity based on risk. This control enhances traditional username/password credentials as the sole authentication step for end users. |
| **Data Encryption** | Use of dedicated VPNs, digital signatures and public key infrastructure implemented to encrypt confidential data transmitted over the internet and at rest. |
| **Role Based Access (RBAC)** | Predefined roles to provision user access according to the assigned roles/responsibilities. |
| **Network Isolation** | Extensive safeguards in-place to maintain data integrity. Network segmentation applied to the database and application servers to an environment that has no external exposure. |
| **Endpoint Protection** | Controls in place to detect and prevent unauthorized transmission of confidential data externally. Endpoint security on employee workstations to include personal firewall, antivirus and malware detection, internet proxy and data loss prevention and servers to include host based intrusion prevention (on internet facing only) and anti-virus. |
| **Background investigations on all employees** | Pre-employment screening including work history, criminal background, identity, social security, address trace, education verification, drug screening and Office of Foreign Asset Control (OFAC). |

## CONTACT US TODAY

**For more information:**
moreinfo@equifax.com
800-888-8277
www.equifaxworkforce.com