EQUIFAX®

Global Security from Equifax

Trusted Stewards of Data

Security is Our Priority

Our tiered operational structure integrates critical security functions of engineering, operations, compliance investigations and credentialing. This helps extend our security protection and controls beyond our organization to include our third-party suppliers as well.

Global Security from Equifax

Corporate Security	■ Physical Security ■ Fusion Center ■ Safety and Defensive Travel Program ■ Insider Threat ■ Internal Investigations ■ Credentialing ■ Fraud Monitoring and Fraud Investigations ■ Law Enforcement Liaison and Support
Business Resilience	■ Business Continuity ■ Crisis Management ■ Third Party Risk ■ Client and Reseller FCRA Audits ■ Questionnaires, RFPs ■ Contract Review ■ Privacy Operations ■ PCI, ISO27001, FISMA Strategy and Certifications
Regional Security	■ Business Liaison to/from Security ■ Business Unit/Country Champion ■ Policies and Standards ■ Security Education and Awareness ■ Business Advisements ■ Mergers and Acquisitions ■ Client Audits
Cyber Threat Center	■ Intelligence Gathering ■ Vulnerability Management ■ Countermeasures ■ Cyber Security Strategy ■ Security Operations

If you're not ahead of security risk, you're behind it. At Equifax, that's what drives us to constantly challenge our internal teams to think about data security differently, connect the dots and look for the bigger picture, the next trend or hidden vulnerability.

Our pre-emptive approach is carefully designed to provide our customers with peace of mind that's backed by a variety of administrative, physical and technical controls to better protect data from every angle. It's comprehensive, data-driven and well-vetted throughout our organization to ensure that Equifax is secure, and growing stronger, even more secure every day.

We Leave Nothing to Chance

In security, it's often what you don't see — the hidden patterns, connections and inconsistencies — that can cause trouble, fast. Knowing that, Global Security from Equifax provides a strategic framework and guiding principles for a 360-degree stronghold that helps us quickly detect, prevent and respond to security issues.

We Carefully Monitor Our Access Points

The most visible security touchpoint is physical access. At every Equifax facility, we follow strict security protocols. Access controls are implemented and monitored at multiple levels by our state of the art 24x7x365 Fusion Center including badged access to facilities, real-time video surveillance of all critical facilities, immediate response to events both locally and regionally, 24/7 security guards, intrusion detection systems and more.

The Equifax environment is protected using a layered security approach that leverages a variety of personnel, processes and technology including:

- Endpoint security controls such as laptop and email encryption, antivirus, anti-malware, host-based firewalls, two-factor authentication, forensics tools and more
- Network controls such as firewalls, web application firewalls, multi-factor authentication, internal network segmentation, vulnerability scanning/remediation, proxies and more

"Need-to-know" principles govern access to systems and data for employees, partners and contractors, while "permissible purpose" controls ensure appropriate access to sensitive, consumer data.

External parties with access to Equifax systems or data are closely evaluated for security risk prior to working with Equifax and routinely re-evaluated using a tiered risk prioritization model. Similarly, customers undergo credentialing processes to evaluate potential fraud and security risk, and ensure legitimacy.

All Equifax employees with access to data, systems and facilities undergo in-depth background screening every five years, unless prohibited by law. Further, all internal and remote employee access to Equifax systems and data is continuously monitored.

Cyber Security is a Dedicated Focus

Malicious online security risk is evolving at an alarming rate. To address this issue, we created a Cyber Threat Center as a separate, dedicated group within Global Security. The core focus of this highly specialized team is to:

- Identify and mitigate active threats
- Model new and emerging threats to better understand future risk paths and trajectories
- Support investigations around a variety of situations such as insider threat, external bad actors, fraud and more

This group constantly asks the hard questions. What data do we have that's most valuable to others? Who has access to that data, and are our technical controls working? What's the baseline for "normal," what's changed and what doesn't look right?

The answers they get, paired with market-leading Equifax technology and automated analytics, dramatically expand our view of risk and provide greater, more predictive insight into current and future security issues.

We're "Always On"

Within every organization, unexpected events such as natural disasters can put operational security to the test. Equifax follows a systematic approach and testing methodology modeled after the standard Professional Practices endorsed by Disaster Recovery Institute (DRI) International.

Pairing these practices with the expertise of our well-qualified business continuity professionals helps safeguard the reputation of Equifax and our customers by sufficiently identifying threats and their associated risk potential under extenuating business conditions. In other words, our global security protocols are designed to remain effective, intact and always on.

In a typical day, our Cyber Threat Center:

2.5	Billion Logs Captured
50k	Events/second Monitored
2,200	Security Device Health Checks
43k	Domains Analyzed
250	Intel Forums Queried

ISO27001

PCI

FISMA

CISSP

CIPP

CISM

CISA

CFE

CEH

We Engage Our Employees, Our Industry and the Community

Knowing that security today is more complex than ever before, we are driven to constantly enrich our proprietary expertise and industry connections.

Talent for our high-performance Global Security team is carefully chosen and cultivated. Between our professional development programs, internal promotion policy and our university recruiting programs located inside and outside the U.S., we hire and retain some of the most skilled and experienced IT and security professionals from around the world. This enables us to put the right people with the right knowledge in the right place to optimize our security performance.

Equifax also maintains a multitude of security credentials including ISO 27001-global certification, FISMA certification of several core systems, SOC2, Type 2 reports and PCI certification. We take pride in our academic research initiatives and our strong commitment to the security profession. Likewise, we actively engage our business customers by participating in customer advisory boards, security roundtable working groups, anonymized threat indicator sharing, customer audits, industry forums and more.

Community engagement is also routinely facilitated through participation at local, city and state security forums, and with law enforcement agencies.

We're Always Innovating and Looking Ahead

Through innovation and collaboration, Equifax is pushing ever deeper into the landscape of information security. As our scope of security responsibility extends to more markets and new business relationships, we are building strong associations with key players and thought leaders in the technology security industry, academia and regulatory spheres.

Now more than ever, our Global Security is facing forward, committed to advancing the powerful information safeguards that keep and grow the trust of our customers and consumers.

❯ **CONTACT US TODAY**

For more information, contact your Equifax representative.

Copyright © 2017, Equifax Inc., Atlanta, Georgia. All rights reserved. Equifax and EFX are registered trademarks of Equifax Inc.