# Security Overview

## BlackBerry Corporate Infrastructure

Published: 2015-04-23
SWD-20150423095908892

# Contents

# Introduction

1

BlackBerry is synonymous with security. BlackBerry products, from smartphones, to service environments, to enterprise software, are engineered from the ground up with security built into every layer. That's why BlackBerry is the preferred solution for customers that require absolute confidence in the security of their data.

But secure design doesn't happen in a vacuum. Products must be conceptualized, designed, implemented, and managed in an environment that fosters similar expectations. This guide provides a detailed look at the environment that we make BlackBerry products in. It covers the internal security of BlackBerry Ltd. itself, and the tools, techniques, processes, and people that let us bring you these incredible products.

For more information about the security of BlackBerry products and services, see the BlackBerry Security Overview.

# History

2

BlackBerry has an established record of integrating secure practices. In 2002, BlackBerry was one of the first organizations in North America to receive accreditation against the *BS7799 Security Standard*. This standard was later adopted by the International Standards Organization as *ISO/IEC 27001:2005* and, most recently, *ISO/IEC 27001:2013*.

ISO/IEC 27001 provides a model for establishing an information security management system (ISMS), which aligns people, resources, and controls, to create a series of measurable security practices to protect information assets. BlackBerry uses BSI Group, an independent, external company, to certify and validate that BlackBerry has an appropriate ISMS in place for the processes, systems, and infrastructure that support BlackBerry services. The BlackBerry ISMS Certificate of Registration is publicly available on the BlackBerry website. BlackBerry is also certified as Payment Card Industry Data Security Standard (PCI DSS) compliant and continues to work with external assessors such as Trustwave and Herjavec Group to maintain compliance in this area.

# BlackBerry policies

3

BlackBerry has a broad range of policies, standards, and guidelines that address all aspects of corporate security. These policies apply to all employees of BlackBerry at all levels and include (but are not limited to) such topics as:

- acceptable use of BlackBerry systems
- information classification and handling
- personnel and human resources
- privacy and records management
- asset management
- access control
- physical and environmental security
- operations and communications
- network security management
- systems development, acquisition, and maintenance
- third-party management
- incident management and response
- remote and mobile computing
- business continuity and disaster recovery
- compliance

These policies address the laws, rules, and practices that regulate how BlackBerry develops, manages, protects, and distributes confidential information globally. These corporate security policies are:

- vetted, approved, and enforced by executive management
- reviewed and updated as necessary to respond to the changing threat landscape and legislative/regulatory compliance requirements

Policies are reviewed on a recurring basis, at least annually. They are communicated to all employees and are always available on our corporate intranet. On an annual basis, all employees are required to affirm adherence to these policies in the *BlackBerry Code of Business Standards and Principles* document, which also addresses employee confidentiality commitments and a code of conduct.

# Security organizations

4

BlackBerry has several global security teams that work closely to ensure a cohesive and consistent security program.

## Corporate Security & Risk

The Corporate Security & Risk team is responsible for the security governance program at BlackBerry. This team develops policies, standards, and guidelines that govern our Security Management System (SMS), drives adoption of security controls, and ensures that architecture and processes remain compliant with security policies through regular assessments of BlackBerry systems and third-party service providers. Risks that exceed a specific threshold are subject to executive risk review and management processes.

The Corporate Security & Risk team monitors and responds to threats to our enterprise and service environments using industry standard technologies and scans hosts for known vulnerabilities. They regularly engage with external experts to conduct independent tests and/or validation of existing system security controls for BlackBerry Ltd. systems and applications.

The Corporate Security & Risk team is also responsible for administering awareness training to all employees at BlackBerry and regularly conducts awareness campaigns to test employee adoption and retention of security practices (for example, internal phishing campaigns and formal tests).

## Physical Security

The BlackBerry Physical Security team implements and maintains all aspects of physical security. This organization also maintains close relationships with local emergency services and authorities to ensure a timely response in the event of a security incident.

## Cyber Forensics & Investigations

The Cyber Forensics & Investigations team specializes in conducting forensic examinations. The team has built and maintained an enterprise forensics capability over the last decade using a variety of commercial and open-source tools. Following industry standards and best practices, the team acquires and examines data from multiple sources of digital media from anywhere across the enterprise.

# Risk, Performance, & Audit

The Risk, Performance, & Audit team, which reports directly to the Audit and Risk Management Committee of the Board of Directors, provides another layer of oversight for BlackBerry. This reporting structure affords us an additional layer of independence when evaluating risks and controls for the company. This team also participates in areas of fraud and ethics investigations.

# Virtual Incident Response

BlackBerry has established a Virtual Incident Response Team (VIRT). This is a cross-functional team of experts from throughout the organization who are responsible for responding to incidents that impact, or have the potential to impact, our enterprise environment. This team is able to rapidly and effectively respond to emerging incidents and provide the guidance and tools necessary to protect our systems and devices.

# Privacy

BlackBerry has a dedicated Privacy team that, in partnership with the Corporate Security & Risk team, assesses our technical and administrative security controls to ensure compliance with international legislative requirements governing privacy matters.

BlackBerry complies with data protection and privacy laws concerning the collection, use, storage, transfer, and disclosure of data containing personally identifiable information (PII), including the EU Data Protection Directive.

Our commitment to customer privacy is detailed in our Privacy Policy and the INSIDE BlackBerry Blog.

# Physical and environmental security

5

## Physical security

All BlackBerry facilities and information resources have physical access controls in place to protect them from unauthorized access and safeguard against environmental hazards.

All areas of BlackBerry are assigned a zone rating based on the sensitivity of the activity, systems, or data in use. These zones dictate the types and level of controls that must be implemented. Access to specific security zones is controlled through a global enterprise access management system that requires unique access badges for each person. Access can be updated or revoked globally and immediately. These badges and access are audited on an annual basis and anytime that employees change roles. Access to specific areas is restricted based on job function, and some areas are prohibited to even our most senior executives.

BlackBerry makes wide use of glass break detectors, internal and external video surveillance on all entry/exit points and key areas within the facilities, and optical gates to manage traffic flow. Sensitive areas also use biometric identification, vibration and motion sensors, x-ray machines, and metal detectors.

BlackBerry also employs highly trained security guards that are led and managed by a dedicated internal BlackBerry Physical Security team. Sensitive locations also use crash-rated barriers and fences to prevent vehicles from penetrating the building perimeter.

## Data centers

Operational confidentiality, integrity, and availability are absolutely critical to BlackBerry and to all of our customers. Our data centers are geographically distributed globally, and each facility undergoes a thorough risk assessment. Facilities have multiple redundant power supplies, climate control systems, fire suppression systems, and Internet connections. These environments are monitored 24x7 by a dedicated team, and we regularly test these systems and our ability to fail over to alternate sites.

## Visitors

Visitors are subject to several verifications and procedures before they are granted limited access to any BlackBerry facility. Permission must be provided in advance by an authorized individual, and visitors are required to identify themselves using government-issued identification. All visitors are required to agree to a set of documented terms and conditions before they are provided a temporary, visually distinct, visitor's badge. These badges do not provide access to BlackBerry facilities, but serve to identify the individual as a visitor and not an employee. Employees are required to escort their visitors at all times.

# Human resources

6

All BlackBerry employees, external contractors, security guards, janitorial services, and so on, are subject to background screening before an offer of employment. We have engaged with several third-party service providers who specialize in this area. Background screening of candidates includes checking their social presence, education, certifications, and prior work experience, in addition to performing criminal and financial checks. Successful candidates are required to sign non-disclosure agreements and code of conduct agreements as a condition of hiring.

Employees are trained in both general and specific information-security procedures and the correct use of information-processing facilities to minimize the likelihood of a security breach through our Security Essentials training, regular awareness communications, and targeted security campaigns. Our awareness program emphasizes that security and privacy are part of every employee's role at BlackBerry and that every employee has an obligation to act in a manner consistent with our security goals.

# Access control

7

BlackBerry uses a variety of tools and systems to ensure that all activities are attributable and nonrepudiable.

## Authentication

All employees at BlackBerry have unique user IDs to ensure that any access to BlackBerry systems can be attributed to them. The mechanisms used to validate an individual's authentication credentials include strong passwords, two-factor authentication, certificates, and biometric technologies.

## Authorization

BlackBerry gives access to information, systems, and facilities on a need-to-know and job-specific (role-based) basis. Ownership of assets is assigned to specific teams and individuals, and a formal process for requesting, approving, and granting access is in place. Access can be limited to a specific time window and then automatically revoked using automated tools and workflows.

System administrators are assigned administrative accounts using least-privilege access. All administrative access is logged, and automated reports and alerts are generated when these accounts are used.

## Termination procedures

At the end of an individual's employment with BlackBerry, their user ID is immediately terminated. BlackBerry runs daily reports to ensure that terminated employees no longer have access to BlackBerry systems and facilities.

# Communications and operations management

8

## Asset management

BlackBerry has an approved policy to maintain inventory of hardware, software, information assets, and physical assets. Information assets are risk-classified based on criticality and/or sensitivity of information. Assets are rated based on legislative, regulatory, and/or policy requirements, and on sensitivity and impact considerations in the event of a security incident.

## Infrastructure security

BlackBerry uses a variety of technologies to ensure the confidentiality, integrity, and availability of our systems and data.

Servers and gateways are protected through a combination of antivirus software, enhanced monitoring, redundancy, segregation, intrusion-detection, and intrusion-prevention systems. Workstations have antivirus and disk encryption software installed and host-based firewalls enabled.

BlackBerry uses a variety of firewall technology solutions for stateful packet inspection. User and service activity is tracked, monitored, and logged. Logs are regularly reviewed for unsuccessful logins, access violations, and privileged access.

Baseline network-security monitoring is done through the deployment of network intrusion detection and prevention systems. These systems run on the network and at the perimeter with alerting mechanisms to detect potential security breaches. Signatures are updated at least once a week.

BlackBerry implements multiple layers of control to protect against distributed denial of service (DDoS) attacks. We have deployed both local and cloud-based DDoS mitigation technology across our systems.

BlackBerry also uses content filtering software, data leakage protection (DLP), and advanced persistent threat (APT) tools to monitor for unusual traffic and issue alerts for investigation and response.

## Media disposal

When no longer required, all media is wiped in accordance with formal processes and tools designed in compliance with NIST Special Publication 800-88 rev 1. Media that is not functioning or is at the end of its lifecycle must be destroyed.

# Vulnerability and patch management

To minimize the risks from known threats and vulnerabilities, BlackBerry has implemented a robust vulnerability and patch management process. We continuously monitor public and private sources in order to understand and respond to new vulnerabilities and methods of attack. We have close relationships with partners and receive notifications for any new security vulnerabilities to be assessed and remediated.

BlackBerry regularly examines our environment for social and technical vulnerabilities and uses a combination of tools for vulnerability and penetration testing. We regularly engage with third parties to conduct independent testing of our systems and to externally validate our own internal processes and tools.

When a vulnerability is identified, BlackBerry works with asset owners to determine the appropriate response and track the issue until it's resolved. BlackBerry follows a standard automated patching process, using multiple software tools as appropriate, for each OS and application.

# Systems development and maintenance

9

Secure development practices and validation are built into all phases of the systems management lifecycle. Our security teams are fully integrated into development team processes and provide education and reviews throughout.

BlackBerry uses a risk-based approach to ensure appropriate controls are identified and implemented. Where new technology is being developed, the Corporate Security & Risk team investigates potential impacts and shares this information within the development community. They also work closely with system owners to develop security baselines for each component of the infrastructure.

BlackBerry uses a combination of automated and manual code verification procedures using industry standard tools and processes, and performs vulnerability assessments to ensure appropriate security hardening has been implemented.

Finally, the Corporate Security & Risk team completes a security risk assessment and communicates residual risk so that the necessary risk management decisions and approvals are understood by system owners and business executives.

# Disaster recovery and business continuity

10

BlackBerry's dedicated business continuity measures are part of our commitment to providing our customers with the dependability they have come to expect from the BlackBerry platform. Our business continuity management group delivers an industry standards-based framework for our global operations. Our business continuity program includes a range of initiatives that focus on three main areas:

- disaster recovery
- incident and crisis management
- business continuity

## Disaster recovery

Disaster recovery is accomplished by developing and maintaining accurate and up-to-date recovery capabilities and procedures, and by rehearsing and testing for critical technology services. In addition, resiliency is designed into critical BlackBerry Infrastructure components to ensure minimal impairment to the service experience during any failure events or maintenance activities. Disaster recovery testing for the BlackBerry Infrastructure is done regularly using a combination of walkthroughs, simulated exercises, and production testing.

## Incident and crisis management

Incident and crisis management involves a coordinated response to a major event. This includes standardized procedures that outline the roles and responsibilities during an incident to provide prompt handling of tasks and the steps to be taken during an incident, including identification, classification, escalation, diagnosis, resolution, recovery, and post-incident review.

## Business continuity

Business continuity plans concentrate on critical day-to-day business operations. These plans include identifying critical operational and support teams required to maintain BlackBerry functions if an incident occurs that leads to the unavailability of work areas, people, technology, or third parties. Our business continuity program includes the following key elements:

- business impact analysis and strategy development
- development of business continuity plans

- exercising of business continuity plans
- business continuity training and awareness

# Incident response and management

11

BlackBerry has developed a mature incident response process for security incidents that impact the confidentiality, integrity, and availability of BlackBerry assets and data. We use public and private industry sources and analyze security incidents experienced by other organizations. Our processes include communication and escalation protocols with regulatory bodies and government agencies, and automated alert mechanisms for security incidents that are related to physical, infrastructure, and information systems.

All of our incident response plans meet or exceed major industry standards.

# Summary

12

BlackBerry is the gold standard in secure wireless communications. In addition to building industry-leading mobile solutions, BlackBerry operates the world's largest secure mobile network with end-to-end encryption. By implementing rigorous security standards across all of its assets, products, services, network, and infrastructure, BlackBerry offers unmatched security trusted by governments, enterprises, and consumers around the world.

# Legal notice

13