



## **BlackBerry Third Party Outsourced Worker Code of Conduct**

### **Introduction**

The BlackBerry Third Party Outsourced Worker Code of Conduct focuses on important and common compliance and security expectations for all non-BlackBerry employees, contingent workers, and consultants (referred to as "outsourced workers").

You, or your employer, has a contract with BlackBerry that requires you to access BlackBerry systems or facilities to perform work for the benefit of BlackBerry (your "BlackBerry Assignment"). You must comply with your employer's policies in connection with your BlackBerry Assignment.

Even though you are providing services for the benefit of BlackBerry, you are not a BlackBerry Employee.

It is your responsibility to exercise good judgment, conduct business with integrity, comply with applicable laws, and comply with BlackBerry policies related to your BlackBerry Assignment.

All outsourced workers with system access must review the BlackBerry Third Party Outsourced Worker Code of Conduct, print, sign and return the acknowledgement to your employer prior to the start of your assignment with BlackBerry.

### **Ethics Link**

Nothing is more important to BlackBerry than its reputation and its customers and business partners' trust. Your compliance with these guidelines is mandatory. If you have any questions or concerns, contact your employer or your BlackBerry business contact.

Any suspected ethics and compliance violation must be reported. There are many ways for you to report concerns, including through the BlackBerry Integrity & Compliance Office ([integrity@blackberry.com](mailto:integrity@blackberry.com)) or through [BlackBerry EthicsLink](#). BlackBerry EthicsLink permits you to report concerns directly to the Audit Committee of the Board of Directors.

You are not discouraged or prohibited from disclosing violations of law or instances of fraud, waste or abuse to appropriate government authorities or law enforcement agencies.

Retaliation in any form against anyone who makes a good faith report of suspected illegal or unethical conduct or participated in an investigation of a reported misconduct is a violation of the BS&P and will not be tolerated by BlackBerry. It does not matter whether the specific circumstances reported amount to misconduct. Consistent with legal requirements, the identity of anyone who provides information will be kept confidential.

### **Accurate Records/ Reporting of Work Time and Expenses**

You must maintain accurate books and records. By submitting your time, you are representing that you have accurately reported your time and that you have not performed any work not reported.

## Fraud and Corrupt Practices

At all times, you are required to conduct yourself in accordance with the highest standards of honesty, integrity, and fair dealing:

- The use of BlackBerry funds or assets for any unethical or illegal purpose is strictly prohibited.
- You are never authorized to take any action, make any payment, or make any promises to anyone in government, any political parties or candidates for office, or to private persons for the purpose of obtaining or retaining business for BlackBerry, unless expressly approved by BlackBerry.
- You are not permitted to receive any gifts, entertainment and/or other business courtesies related to your BlackBerry assignment, except as provided by your employer, when performing services for BlackBerry.
- You are not permitted to provide gifts, entertainment, or anything else of value to any government official or employee when performing services for BlackBerry.
- If you are employed by, or have any other role in any federal, state, provincial, local or foreign government or government-owned entity, you must fully disclose this in writing to your employer and BlackBerry before engaging in any work for BlackBerry.
- If you believe that any fraud or unethical activity has occurred relating to your BlackBerry Assignment, you should immediately report the matter to BlackBerry's Office of Integrity & Compliance ([integrity@blackberry.com](mailto:integrity@blackberry.com)) or [BlackBerry EthicsLink](#).

## FAIR COMPETITION

You should not make unfair, misleading, or inaccurate comparisons with the products and services of BlackBerry's competitors.

## Cooperation with Audits and Investigations

From time to time, BlackBerry or authorized third parties may conduct audits or investigations relating to your assignment. Except as otherwise agreed by your employer and BlackBerry, you must cooperate completely in any investigation relating to your BlackBerry Assignment. In connection with any such investigation, you must be honest and forthcoming and provide the investigator with full, accurate, timely, and truthful information. You must never misrepresent facts or fail to disclose facts. You must never interfere with or obstruct an investigation conducted by BlackBerry, by any third party on its behalf, or any government agency.

## Document Retention and Disposal

During the normal course of your BlackBerry Assignment, you may be responsible for creating, using, storing, and disposing of BlackBerry records. You will be instructed by BlackBerry if you are subject to specific document retention requirements.



## Conflict of Interest

As an outsourced worker, you must avoid engaging in any business activity that would conflict or interfere with your performance of your BlackBerry Assignment. You are required to disclose any potential conflict of interest to your BlackBerry manager, your employer, and BlackBerry's Office of Integrity and Compliance at [integrity@blackberry.com](mailto:integrity@blackberry.com).

## Insider Trading:

At times during your assignment with BlackBerry, you may have access to BlackBerry business information that an investor could consider important in deciding whether to buy, sell or hold securities that have not been made public. Applicable laws and BlackBerry policy prohibit insiders from trading or influencing the trade of BlackBerry securities while possessing material information that has not been made generally available to the public.

## Confidential Information

You are not to disclose BlackBerry Confidential Information.

Much of the information available to you during your BlackBerry Assignment is confidential or proprietary. This information, not generally available to the public, includes BlackBerry technical information, business and marketing data and plans, financial data, internal e-mail communications, information about customers, existing and future product information and any other information generally considered confidential.

You are not to discuss such information in public places where others may overhear you, or on blogs or social media networks. Discussion with co-workers, or BlackBerry suppliers or business partners or their contractors that involve confidential or proprietary information must be on a need to know only basis.

You must comply with all terms of the non-disclosure agreement between your employer and BlackBerry.

## Privacy

Depending on your role it may be possible that you may have access to BlackBerry employee or customer personal information. Personal information includes any information relating to an identified or identifiable natural person.

An identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. For detailed information about what personal information BlackBerry collects and processes, see BlackBerry's [Privacy Policy](#).

You are required to handle personal information responsibly, in accordance with its security classification and only use, process, or disclose such data within the terms of your BlackBerry Assignment. For questions related to privacy at BlackBerry or to disclose a privacy-related incident, contact [PrivacyOffice@blackberry.com](mailto:PrivacyOffice@blackberry.com).

Failure to engage in proper handling of personal information could result in disciplinary action, up to and including termination of your assignment with BlackBerry.

## Inclusive Workplace Culture

Since the early days of BlackBerry, our customers have trusted BlackBerry to provide the most reliable products and services. We have kept this trust over the years by conducting our business ethically and responsibly. Our business depends on your commitment to integrity. Just as this applies to how we treat our customers; it also depends on how we treat each other.

- Physical conduct, written or spoken communication, or videos and picture can all be inappropriate depending on the action or content.
- Commentary about race, disability, religion, sex, gender identity, marital status, sexual orientation, or pregnancy – depending on the content – can constitute inappropriate harassment. Be respectful and consider others before you act or speak.
- Sexual harassment can include such acts as unwelcome sexual advances and requests for sexual favors or other physical or verbal conduct of a sexual nature. Such conduct is never acceptable.

While the legal definition of harassment varies from country to country, at BlackBerry we reject any unwelcome conduct that has the purpose, or can reasonably be construed to have the effect, of creating an intimidating, offensive or hostile work environment.

To this end, we must all promote and protect a tolerant and inclusive workplace. This requires mutual respect, and our professional relationships must be free from any form of harassment.

BlackBerry embraces diversity in all forms, and we rely on each other to promote an inclusive workplace culture.

## Social Engineering

Social engineering is the deliberate application of deceitful techniques designed to manipulate someone into divulging information or performing an action that may result in the release of that information.

As an outsourced worker, you may be the target of a social engineering attack against BlackBerry. You always need to be aware of people trying to obtain confidential information. This includes social engineering initiatives involving face-to-face interactions, phone calls, and via emails or websites.

Report any suspected social engineering attempts to the Security Operations Center by sending an email to [soc@blackberry.com](mailto:soc@blackberry.com) or visit [go/security](http://go/security).

## Insider Threats

An insider threat can potentially cause harm to BlackBerry (either intentionally or unintentionally). An insider is a current or former employee, outsourced worker, or business partner that has or had access to BlackBerry information.

As a BlackBerry outsourced worker, you must be vigilant of behaviors that may be indicators of insider threat.



## Meals, Gifts and Entertainment

Global commercial and official bribery and anti-corruption laws prohibit offering or receiving meals, gifts, or entertainment to improperly influence the recipient.

As an outsourced worker, you must comply with all bribery and anti-corruption laws where you do business.

## BlackBerry User ID and Password

As an outsource worker with BlackBerry system access, you will be assigned a user ID. This ID is unique to you. Do not share your ID or password with anyone and do not write your password down. Protecting your ID and password is critical to protect yourself and BlackBerry against malicious activities.

## Security Access Badges

Physical access control is one of the most effective corporate security controls.

If you are working from or visiting a BlackBerry office, you will be issued a security access badge. This badge must always be visible and is provisioned with access to the floors and spaces that are required for your BlackBerry assignment.

## Secure Workspace and Disposal

If working at a BlackBerry office, you will be allocated a workspace where you will likely spend most of your time. Ensure that this workspace is clear of sensitive information, lock your computer when you step away from your desk, and ensure all confidential documentation is stored securely or disposed of using secure shred bins.

## Acceptable Use of BlackBerry Assets

BlackBerry assets and information are to be used for legitimate business purposes only. Personal use of BlackBerry assets such as company email, or internet connections is not permitted. BlackBerry information is never to be stored on personal laptops or tablets.

BlackBerry assets must never be used to access or share information deemed inappropriate for a workplace setting. Any outsourced worker who downloads or views inappropriate material may be terminated.

When using BlackBerry assets, the information sent or received is not private and content may be monitored on a routine basis. Unless prohibited by local law, BlackBerry may monitor your use of company assets to make sure it is consistent with the principles set forth in the BlackBerry Third-Party Outsourced Worker Code of Conduct.

## Network Connectivity and BlackBerry Owned Endpoints

Safeguards have been developed to ensure the reliability of BlackBerry network infrastructure, software, and services. BlackBerry endpoints are configured to specific standards and with approved software. All software on BlackBerry provided equipment must be fully licensed to BlackBerry.

If you are assigned a BlackBerry managed endpoint, you must connect to the BlackBerry network by the approved endpoint configuration and network connectivity solution. Any changes to hardware or software configuration will require the outsourced partner to discuss proposed changes with their BlackBerry business contact and follow the BlackBerry change request procedure.



If you have not been assigned a BlackBerry endpoint, specific direction regarding endpoint configuration and network connectivity will need to be followed. Please discuss with your BlackBerry business contact.

If at any time, you have a reasonable suspicion of a security incident that may impact BlackBerry materials or systems, you must notify BlackBerry Security Operations Center at [soc@blackberry.com](mailto:soc@blackberry.com), 1-877-746-5831 x79997.

## Secure Development Lifecycle

Many outsourced roles at BlackBerry assist with the development or testing of BlackBerry products and services. If your assignment includes such responsibilities, you need to be aware of BlackBerry's Secure Development Lifecycle policy and associated practices.

As a software producer, BlackBerry has a critical role to play in protecting the software supply chain of our customers. When purchasing BlackBerry's products, customers place their trust in our ability to safeguard their data, employees, and technology. Customers trust BlackBerry to incorporate industry best security practices into all phases of our development lifecycle, and throughout our products' supported lifetime.

BlackBerry has a Secure Development Lifecycle policy which outlines the foundational security practices which must occur to ensure we deliver well-secured software to our customers. This policy is based on industry standards such as the NIST Secure Software Development Framework, and helps BlackBerry meet the compliance and regulatory programs of the markets we serve. The SDL policy applies to all BlackBerry products – from desktop and mobile clients, to embedded solutions, to cloud-based Software-as-a-Service offerings.

If you have any questions about BlackBerry's secure development lifecycle, please discuss with your BlackBerry business contact.

## Disclosure of Developments

Any Development should be your original work, and no part of it should include the copyrighted work of any other person, unless you have the copyright owner and BlackBerry's or your employer's prior written approval to do so. If you believe that any IP should be considered an "excluded development", have any questions about the use and disclosure of BlackBerry's and third parties' IP, or have any other questions relating to IP, contact BlackBerry's Office of Integrity & Compliance at [integrity@blackberry.com](mailto:integrity@blackberry.com).

## Reporting Security Incidents and Insider Threats

Security is the responsibility of everyone, including BlackBerry outsourced workers. We all have an obligation to report suspected security incidents including Insider Threats.

Contact the Security Operations Center for any of the following:

- Concerns of an Insider Threat
- Potential data loss or spillage of classified or sensitive data
- Lost or stolen items, such as laptops, BlackBerry access badges, and non-public documents



- Being asked for your BlackBerry laptop or password by anyone
- Someone requesting access to sensitive company resources not related to job duties or responsibilities
- Unauthorized or inappropriate use of the BlackBerry network and systems
- Unauthorized access to secure areas of BlackBerry buildings
- Mishandling or misusing BlackBerry sensitive and proprietary information
- Disgruntled employees or former employees
- Employees or outsourced workers being irresponsible with BlackBerry information and property
- Irresponsible social media behavior
- Use of unauthorized software and devices
- Encounters with suspected social engineering attempts

Contact the Security Operations Centre to report an incident by sending an email to [soc@blackberry.com](mailto:soc@blackberry.com).