



Social Media Policy - Summary

The Brink's Social Media Policy applies to all Brink's U.S. employees, and applies to all forms of electronic communications. The purpose of this policy is to clarify that the responsibilities of Brink's employees relating to confidentiality, security, off-duty conduct and compliance with Company policies are applicable to their on and off-duty use of the Internet and similar electronic communication platforms. This policy is not intended to interfere with the free flow of information between employees. The Social Media Policy addresses the following issues:

Confidentiality. The Brink's Business Code of Ethics directs that all employees keep confidential all information about Company business activities that is not common knowledge. Disclosing confidential information in social media can create significant security risks. The unauthorized posting, discussion or forwarding of any Brink's (or customer, vendor or competitor) related information such as written materials, photos, videos and audio files containing confidential information, or discussions or posting of Brink's business information or activities in social media not controlled by Brink's is prohibited. Confidentiality requirements do not apply to Brink's employees' wages or other terms and conditions of employment.

Unauthorized Marketing. The creation of unauthorized postings or websites in connection with the promotion or sale of Brink's services is not allowed. Likewise, employees are not to use Brink's logos or trademarks or the logos and trademarks of others without authorization. Employees are required to disclose their connection with Brink's in all postings in which the employee discusses or recommends Brink's services, and is to make it clear the opinions are their own and do not necessarily reflect Brink's opinions.

Employment. Use of social media for the purpose of recruiting personnel must be coordinated through and have the approval of Human Resources. Job references for current or former Brink's employees on employment or networking websites is prohibited. The Internet should not be used in conducting pre-hire background investigations.

Privacy. Posting information, personal data, pictures or videos of customers, vendors, suppliers or employees on social media sites is not allowed.

IT Resources. The Brink's Information Technology Department will deny access on Brink's systems to certain social media sites. Employees should have no expectation of privacy when accessing social media from Brink's equipment.

Discipline. Employees who violate this policy will be subject to appropriate disciplinary action or other remedial measures up to and including termination of employment, if warranted under the circumstances and permissible under applicable law, collective agreements and individual agreements.

NOTE: This summary is not meant as a substitute for the Brink's Social Media Policy. For complete requirements on social media conduct, employees should refer to the Brink's Social Media Policy itself.

1.0 PURPOSE

The purpose of this policy is to set forth the responsibilities of Brink's employees relating to confidentiality, security, off-duty conduct and compliance with other Brink's rules and policies applicable to their on- and off-duty use of the Internet and similar electronic communication platforms.

2.0 SCOPE

This policy applies to all Brink's employees worldwide. The term "Country" refers to the Brink's entity operating within a specific country. Examples of communication platforms stated in this policy are not intended to be exhaustive, and the rules stated in this policy apply to all forms of electronic communications including but not limited to:

- Social networking sites (e.g., Facebook, MySpace, Friendster, LinkedIn),
- Video and photo-sharing websites (e.g., Flickr, YouTube),
- Micro-blogging sites (e.g., Twitter),
- Blogs (e.g., corporate blogs, personal blogs, media-hosted blogs),
- Forums and discussion boards (e.g., Yahoo! groups, Google groups),
- Collaborative publishing (e.g., Wikipedia).

Compliance with this policy is an expectation of employment subject to local legal requirements.

3.0 INTERPRETATION AND ADMINISTRATION

The interpretation and administration of this policy shall be the responsibility of the Legal and Human Resources Departments for each Brink's Country.

4.0 POLICY**A. The Confidentiality and Security Obligations of Brink's Employees Apply to On-Line Activities**

Among the most important responsibilities of a Brink's employee is confidentiality. The Brink's Business Code of Ethics clearly states that "...all employees, officers and directors keep confidential all information about Company operations and business activities that has not been made public or that is not common knowledge..." The type of information which is considered confidential is described in the Brink's Business Code of Ethics.

These responsibilities concerning confidentiality are of particular importance with regard to information posted on the Internet, websites, blogs, chat rooms, social networking sites (ex. Facebook), email, mass messaging services (ex. Twitter) or other

electronic platforms because of the ease in which information may be transmitted, stored or forwarded and the unknown and virtually unlimited size of its audience. **Further, the posting of seemingly innocuous information or photos, videos or other media concerning Brink's operations, equipment, procedures or liability or that of Brink's customers or vendors could be of an unanticipated benefit or use to the criminal element; resulting in an increased security risk to employees, their families, and the Company.** As a result, the unauthorized posting, discussion or forwarding of any Brink's (or Brink's customer, vendor or competitor) related information or intellectual property, including but not limited to written materials, photos, videos and audio files containing such confidential information, or discussions or posting of Brink's business information or activities on forums, websites, services, chat rooms, social networks, blogs, mass messaging services or platforms not controlled by Brink's is strictly prohibited.

B. Unauthorized Marketing or Promotional Websites or Postings

The creation of unauthorized postings or websites in connection with the promotion or sale of Brink's services can result in unintended disclosures, obligations and/or other legal risks to Brink's. Such unauthorized websites and postings are generally forbidden. Requests for exceptions require the written approval of both Global Marketing and Communications and Brink's Legal Counsel. The unauthorized online use of Brink's logos or trademarks or the logos and trademarks of others is strictly prohibited.

Employees are required to disclose their connection with Brink's in all communications discussing or recommending Brink's, its products or services. In the event of such communications, employees are to make it clear that the opinions are their own and do not necessarily reflect Brink's views or opinions.

C. Disclosure of Affiliation with Brink's

Employees should recognize that there are inherent risks in connection with disclosing their employment by Brink's to a broad audience. **Disclosing this information may make the employee and/or the employee's family a target for the criminal element.**

D. Unauthorized use of Websites or other Online Media for Recruiting, Employment Reference or Background Investigations

The creation of websites, emails, postings, mass messages or other online communications for the purpose of recruiting personnel must be coordinated through, and have the express approval of, Brink's Human Resources Department.

Likewise, employees must comply with Brink's policies governing the provision of employment references for current or former Brink's personnel. In most Countries, policies prohibit anyone other than Human Resources from providing such references. All references for current or former Brink's employees on sites such as LinkedIn are prohibited.

Individuals outside of the Human Resources Department should not attempt to conduct their own background investigations for the purpose of pre-hire screening through the use of search engines, social networking sites, or other Internet resources.

E. Protection of Privacy Rights

Employees may not post, share or disclose any information or personal data regarding Brink's customers, vendors, suppliers or employees without written permission in advance from Human Resources and the affected individuals. For security reasons, employees may not post on social media sites photographs or videos of Brink's customers, vendors, suppliers or employees without written permission in advance from Human Resources and the affected individuals.

F. Brink's Personal Conduct Policies Are Applicable to On-line Activities

Brink's employees should be aware that their personal conduct off duty can impact Brink's. Any adverse public notoriety arising from conduct such as dishonesty or criminal involvement can negatively affect Brink's image and reputation. A Brink's employee's off-duty communications or posting of information, photos, etc. in publicly available electronic platforms, such as web pages, social networking sites, email, blogs, chat rooms, mass messaging services and the like are subject to local laws and policies concerning off duty conduct and can be grounds for disciplinary action in accordance with those laws and policies.

G. Appropriate Use of Brink's Information Technology Resources

Brink's information technology resources are Brink's property solely intended to achieve Brink's business objectives. Inappropriate use is not acceptable. This includes, without limitation, using Brink's systems to post offensive or defamatory material. Proper use is further defined in specific Country policies. The Brink's Information Technology Department will deny access on Brink's systems to certain social media sites, including without limitation, Facebook, Twitter and YouTube. Exceptions will be made only for employees able to clearly demonstrate an important business purpose for access to such sites. Any exception must be approved by the respective Country Head.

H. Discipline and Other Consequences

Employees who violate this Policy will be subject to appropriate disciplinary action or other remedial measures up to and including termination of employment if warranted under the circumstances and permissible under applicable law.

I. No Expectation of Privacy

Employees are reminded that they should have no expectation of privacy when using the Internet or any Internet sites from Brink's electronic equipment. Brink's reserves the right to monitor employee use of the Internet and social media to the extent permissible by applicable law.

J. Reporting Violations of this Policy

Employees who become aware of a violation of this policy should report the violation to their Human Resources Department.

K. Non-Interference with Applicable Laws

This policy is not intended to interfere with the free flow of information between employees and should not be construed to restrict or interfere with any employee's labor law rights or any whistleblower protections provided under law. Additionally, this policy is subject to Country-specific employment laws, data protection and privacy laws, collective and individual agreements. Confidentiality requirements do not apply to Brink's employees' wages or other terms and conditions of employment.

L. Questions about this Policy

Please contact your Legal or Human Resources Department if you have any questions about this Policy.