



BRAINLOOP PRESENTS FIVE BEST PRACTICES TO ENHANCE SECURITY POLICY COMPLIANCE

Boston, December 8, 2009 - Brainloop, the leading supplier of software solutions for high-security management of confidential documents, today issued a white paper that presents how businesses can improve data security without making it difficult for users to do their jobs. The white paper – “Security Policy: Five Keys to User Compliance” – provides specific best practices that businesses can follow to facilitate user productivity while automatically ensuring safe document sharing practices.

“Within each best practice, users are unhindered by security procedures and are able to conduct their work in a transparently secure environment,” said Brainloop President Uli Mittermaier. “The collaboration environment created by sound best practices streamlines processes and improves efficiency, which actually leads users to making it their preferred work environment.”

From the IT perspective, the Brainloop white paper demonstrates how the deployment of a transparently secure work space eliminates the need to force heavy-handed security policies on reluctant users. Policies are enforced automatically, resulting in more consistent adherence to security policy. Because users are able to comply with security policy without even knowing it, the best practices reduce tension between IT and users in addition to producing several business benefits:

- Increased productivity and mobile efficiency
- Improved governance efficiency and regulatory compliance enablement
- Enhanced communication and oversight in collaboration and bidding processes
- Reduced need for costly, time-consuming and inconvenient travel and shipping of physical documents.

The need for a transparent security solution such as the one described in the Brainloop white paper is illustrated in an October 13 article, *Playing the Human Factors*, by Alan Radding that appeared at BusinessFinanceMag.com. Within the article, Radding cites how according to Gartner, 84 percent of data loss incidents involve authorized parties distributing content externally. The article reports that this data point was contained in a CERT Insider Threat Study titled, *Understanding the Risks & Defending the Enterprise*. The cost of that loss, according to 30 percent of survey respondents, exceeded \$500,000.

“Transparent security is a win for everyone, including IT, users and the business,” said Mittermaier. “IT doesn’t have to play a heavy security role and users aren’t burdened with security tasks and therefore are able to focus on their actual work, with the result that the business gets better security and increased productivity.”

To view the Brainloop white paper, “Security Policy: Five Keys to User Compliance,” visit:
<http://tinyurl.com/yh2c5kf>



ABOUT BRAINLOOP

Brainloop, with offices in Boston and Munich, is the leading supplier of software solutions for high-security management of confidential documents. Brainloop Secure Dataroom is a virtual document safe that enables safe filing, editing and distribution of highly confidential documents within a single company, and beyond. All contents are powerfully protected from unauthorized internal or external attacks, and all actions within the data room are documented by a tamper-proof audit trail. Frequent uses include contract negotiations, collecting data and writing up quarterly reports, and any other communication that contains confidential information.

Brainloop Secure Dataroom is used internationally by hundreds of renowned companies including BMW, Deutsche Telekom, Eurocopter, Galileo Industries, Sky (formerly Premiere) and ThyssenKrupp. Leading law firms and investment banks use this solution for the complete life cycle of M&A transactions. Strategic partners of Brainloop are HP, F-I-TS, Microsoft and T-Systems Business Services.

<http://www.brainloop.com>

PRESS CONTACT:

Victor Cruz

MediaPR

vcruz@mediapr.net

(401) 349-3369

Copyright © 2009, Brainloop AG. All rights reserved. All trademarks mentioned in this document are the property of their respective owners.