**FOR IMMEDIATE RELEASE**

**CONTACT: Kevin Froese**

EMAIL: PR@cirius.com

PHONE: 1-888-362-4520, ext. 724

 **Cirius Messaging Announces Encryption Support for New Google DLP Engine***Cirius Adds Secure Email, File Sharing and Message Control for Google for Work Users*

* Cirius’ Secure Messaging supports new Google Data Leakage Protection (DLP) security feature
* Cirius provides an alternative to blocking/modifying private emails by creating rules that allow messages to be encrypted and sent securely
* The solution’s unique cloud architecture makes it simple to set up with cloud-based email such as Google for Work
* Protects confidential and personal information without compromising productivity

Vancouver, BC (December 17, 2015) – Cirius Messaging Inc., a provider of next generation secure collaboration solutions, including cloud-based email encryption, secure file sharing and advanced message control, today announced support for Google’s new Gmail Data Leakage Prevention (DLP) feature, Google DLP. Cirius Secure Messaging augments Google DLP, providing Google for Work users an option to automatically and securely encrypt and send messages and attachments.

Part of the Google for Work application suite, Google DLP prevents users from accidentally or maliciously leaking confidential information, including intellectual property and personally identifiable information such as credit card numbers, via email. Based on pre-set DLP policies, Google’s engine can reject and quarantine prohibited messages or notify the sender that the content requires modification. However, integration with the Cirius Secure Messaging solution provides a rule-based option to encrypt and send messages and attachments securely, rather than blocking or modifying them.

Secure Messaging provides additional features, including message delivery tracking and advanced message controls to lock message forwarding and replies and to recall already-opened messages.

“Google DLP is an important step taken by Google to protect its users’ private information,” said Josef Lara, SVP Business Development, Cirius. “Cirius’ Secure Messaging solution complements Google DLP by offering a productivity-enhancing security feature that facilitates the ability to send confidential emails that otherwise would be blocked, after meeting specific criteria and undergoing encryption.”

Cirius Secure Messaging deploys rapidly and eliminates the need for additional hardware or IT expertise. Equally suitable for SMBs and enterprises, the solution extends full protection to mobile devices, enabling both security and productivity. Key features include:

* Advanced email and file encryption
* Real-time tracking and notification of activities, including when a message is received, read or answered, and the ability to control if it can be forwarded, deleted or printed, through the Delivery Slip
* Advanced message control for ultra-sensitive communications through ReplyFreeze, ForwardFreeze and FYEO (For Your Eyes Only)
* Seamless integration with browser-based webmail clients

All Cirius Secure Messaging features are included in its one low-price subscription. For more information, visit [www.cirius.com](http://www.cirius.com).

**About Cirius**

Cirius is a simplified, next-generation collaboration solution that enables companies to protect and control confidential company data. More than 6,500 customers worldwide in every industry sector depend on Cirius’ innovative platform to communicate securely on any device, control what happens to their messages even after they have been sent, rapidly transfer large files, and prevent data loss.

Cirius Messaging is a cloud-based solution that is easy to use and deploy, yet powerful in its many applications. In this age of growing regulatory oversight and increased pressure to safeguard customer data, Cirius is helping companies gain a competitive edge through better relationships, increased productivity, lower overhead, and a reputation of trust. Visit [www.cirius.com](http://www.cirius.com/) for more information.