This is provided as an example of corporate communications script for the rollout of new security technology only for general informational purposes. Work with your technical, legal and human resources team to tailor this document so that it is accurate and consistent with your cultural, contractual and regulatory requirements.

**Corporate Communications Script**

***Use this script as a blueprint for how to effectively, and transparently, communicate the rollout of new Insider Risk Management technology within your organization.***

**Corporate Communications for the rollout and communication of [Insider Risk Management Technology]**

Information security and data protection are core values at Company X. Securing and protecting our intellectual property and confidential information, as well as that of our employees, contractors, customers, prospects and partners is how we earn and keep customer trust and protect our business reputation. It is also a commitment we make to employees, contractors, customers, prospects and partners, and fundamental to our compliance with regulatory obligations, like HIPAA and GDPR, and certification programs, like PCI and FedRAMP.

Company X also embraces the modern workforce where multiple services can be accessed anywhere. We acknowledge the portability of data and that our most critical assets are our employees and our intellectual property. Merging the need for collaboration and openness to support our tasks, Company X has developed a program to provide visibility to file movement without blocking, classification or intrusive monitoring such as keystroke logging.

We may also use technologies which capture data about your access to and use of Business Systems, such as security software for insider risk management, data loss prevention (DLP), network traffic monitoring, and computer resource utilization monitoring. As an example of how certain technologies work, our security software enables us to capture data and identify particular anomalies in usage of Business Systems, such as attempts to access, download, or transfer particular files or content in violation of Acceptable Use Policy.

Monitoring is only carried out to the extent permitted by law and as appropriate, proportionate and justifiable for the purposes set forth in this policy. Monitoring under this policy will not be used to assess your productivity or performance.

Company X continues to assume positive intent in all cases of investigations or unauthorized file movement.

Please reach out to your [security team/data protection officer] with questions.