Corporate Communications Script

Description:

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

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

Corporate Communications for the rollout of a [Data Protection Technology]

Information security and data protection are embedded in our core values at **[Company Name]**. Securing and protecting our Intellectual Property (IP) and other sensitive corporate data, which includes information pertaining to our employees, contractors,customers, and partners, is how we earn, cultivate, and maintain long-term customer trust. Our collective approach to data protection serves as a commitment we make to our workforce and business partners alike. Proactively safeguarding sensitive corporate data is essential to our success and sustained growth, as well as ensuring we meet our compliance and regulatory obligations.

[Company Name] embraces the modern digital workforce which has proven to be highly distributed, mobile, and flexible. As such, we acknowledge some additional visibility is required to ensure positive and safe work habits for our employees and ensure our data is protected. In order for **[Company Name]** to effectively meet these needs, we aim to merge collaboration, transparency, and openness to support data protection at all levels of our organization. Our data protection approach promotes and supports creativity, innovation, and collaboration across the enterprise by not requiring excessive data classification requirements or generic blocking. We will not engage in intrusive monitoring such as keystroke logging and screen recording or review any personal messages.

We leverage data protection technologies to ensure **[Company Name]** consistently and ethically supports your innovation, collaboration, and professional development. Similarly, we capture data on the use of and access to corporate business systems, such as security software for Insider Risk Management (IRM), Data Loss Prevention (DLP), network traffic monitoring, and computer resource utilization monitoring. Examples of how modern data protection technologies work include the ability to capture data and identify particular anomalies in usage of business systems, such as attempts to access, download, or transfer sensitive files and content unapproved in **[Company Name]** 's Acceptable Use Policy (AUP). Data review is only carried out to the extent permitted by law and as appropriate, proportionate, and justifiable for the purposes set forth in this policy. Data review under this policy will not be used to assess your productivity or performance. **[Company Name]** continues to presume positive intent in all instances of investigations or unauthorized file movement. Please reach out to your [security team or data protection officer] with questions or concerns.