It’s in the employee handbook. That’s the corporate way of saying, “Because I said so!”

Protection of intellectual property (IP) and compliance with regulatory and corporate governance policies is changing the way we communicate and collaborate in our everyday work life. Rules must be put in place to safeguard our proprietary data. Establishing corporate governance policies that dictate—yes, in this case, dictate is correct—is what all savvy organizations are doing to ensure that content is not only protected at rest…in transit…and in use, but also in compliance with all regulations. We all hate being told what to do—but when it comes to cybersecurity, we must follow the rules to mitigate risk.

A well-defined corporate governance operating model touches on management oversight, organizational structure, corporate culture, talent management, and infrastructure—which covers risk oversight policies and procedures, measures and metrics, and enabling IT.

Enterprise data governance policies are designed to:

- Protect sensitive information and intellectual property including passwords and confidential data
- Maintain internet privacy for salary information, Social Security numbers, medical records, legal documents, financial transactions, classified documents, vendor contracts and personal data
- Protect emails and attachments both inside and outside the firewall
- Set protection options by file or document and provide rights to authorized users only
- Prevent sensitive information data leakage and data breaches on the front end rather than invest resources in managing data after a cybersecurity incident has occurred

Meeting governance

Today's focus is on technology governance, which ensures that enterprise information is secure and protected no matter where it travels. Governance includes the standard operating procedures and policies that employees, alliance partners, and customers must follow. Like information security policies drafted as Company Confidential, For Your Eyes Only; privacy policies including HIPAA, GLBA; compliance policies such as SOX, ISO 15489; corporate governance acceptable use policies (AUPs); or internal ad-hoc policies for Project Team Only, which are key to the mission-critical success of business in the digital age. All corporate intellectual property requires the same persistent protection as the information the government deems necessary to protect.

Maintaining compliance

Legislation has been enacted worldwide to provide protection for content—including emails, personally identifiable information (PII), protected health information (PHI) and confidential contractor documents. Governance no goes beyond protection to compliance.

NIST SP 800-171 is designed to reduce the number of reported cyber-attack incidents in federal agencies—with the objective to protect information and communications technology (ICT) systems operated by the federal government and its contractors from cyber threats within the supply chain. The legislation protects sensitive government information from being destroyed, compromised, or stolen in ICT systems between federal agencies and vendors. The Defense Federal Acquisition Regulation Supplement (DFARS) law requires all Department of Defense contractors to become fully compliant by December 31, 2017.

The General Data Protection Regulation (GDPR) law provides guidelines governing the collection and processing of personal information of individuals within the EU. All businesses must comply by May 25, 2018. This regulation affects companies based in the EU and all businesses located throughout the world that process the data of EU citizens.

Content protection + compliance = governance

The challenge is to find a solution that can deliver email and document protection designed with the tools to deliver monitoring and reporting to provide an audit trail that validates regulatory compliance and has an alert system that warns administrators of any misuse of content. Therein lies your technology-driven governance that supports your corporate data governance policies.

The best-case scenario is email and document protection through secure collaboration in a cloud with a private key delivering full control on who can print, forward or edit the synchronized information. Security permissions (or rights) are applied and enforced down to the digital content (emails, documents, pictures) level, resulting in content being persistently protected from misuse—even when opened by any permitted recipient.

For content protection, corporate governance and compliance—GigaCloud™ by GigaTrust™ has you covered delivering persistently protected emails and documents in compliance for collaboration anytime, anywhere, on virtually any device. At

the minimum—put your corporate governance policies into an employee handbook. ‘Cause I said so! And it’s good advice.