titus

by HelpSystems

SOLUTION BRIEF *(Data Classification)*

Titus Config for Remote Work

Empower Remote Employees to Accurately Classify Data and Share Information with Confidence

With employees working remotely, how do you minimize the risk of a data breach or inadvertent exposure of sensitive information? Typically, your security strategy would start with strong network protection, but that isn't as easy when your network is spread out across hundreds if not thousands of remote locations and includes a mish-mash of home-based components.

When working from home, employees rely on email, cloud repositories and other collaboration tools to communicate and share data remotely. Many remote workers connect via less secure Wi-Fi networks than what is available in the office. A lot of data now resides in the cloud where security measures are different from on-premises servers. Corporate VPNs often cannot perform well enough to handle the increased traffic from remote workers, creating productivity bottlenecks. Email and video conferencing have become the primary means of communication, and both have their own security challenges when it comes to sharing information.

Now more than ever you need to protect the data itself. You need to ensure that your data is classified correctly by remote users, that download attempts are being monitored across your remote workforce, and that remote employees have a strong awareness of your data security policies.

If all files and emails are properly classified, you can worry just a little less about a potentially insecure remote infrastructure.

How Titus Can Help

Titus Config for Remote Work is a preconfigured solution that makes it easy for people working from home to safely share files with colleagues, apply data classifications to email and documents according to information handling policies, and prevent data leaks due to human error.

Easily Classify Documents and Files. Titus Config for Remote Work gives users a simple, flexible way to identify sensitive information and enforce classification of documents and emails. The Titus solution enables classification in one of three ways:

- **Manual classification.** Windows users can right click a file on their desktop to classify it or use the Titus classification tools within a document's toolbar. When users hover over the toolbar ribbon within a document, a guidance popup appears to help them choose the appropriate classification.
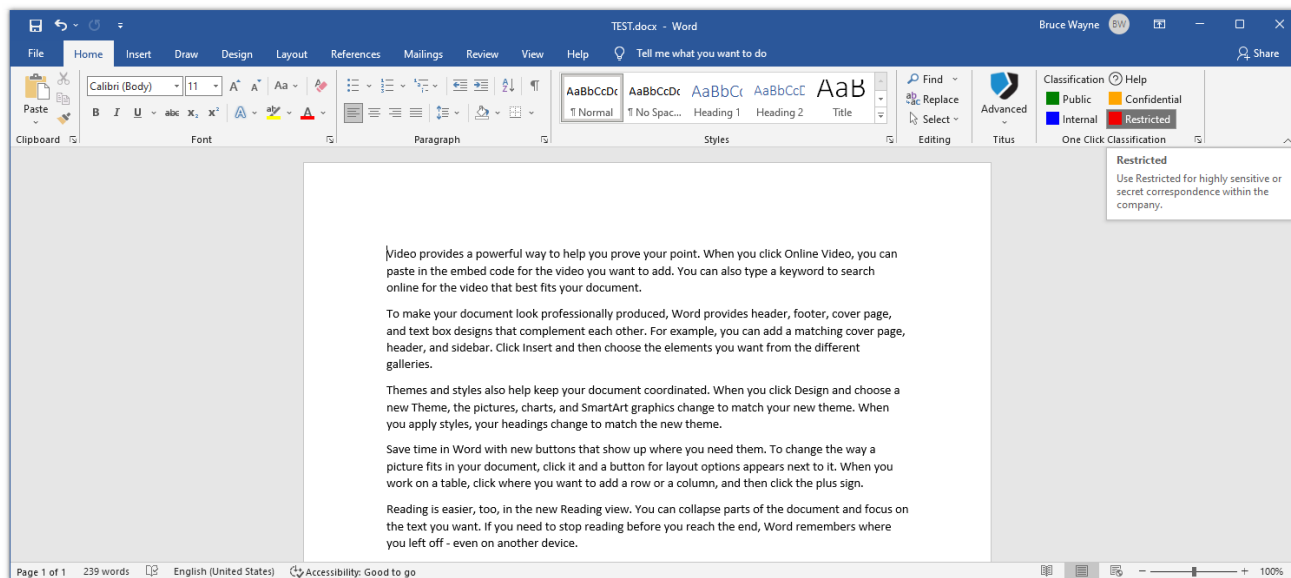
Users can manually select classifications from within a document's toolbar ribbon.

- **Guided classification.** Titus can offer suggestions for how to classify the document based on either step-by-step "Help me Choose" questions in the user interface or intelligent machine learning technology. Users are not forced to use the suggested classifications but must add a classification before saving or sharing a new document.

- **Automatic classification.** Organizations can configure Titus Config for Remote Work to enforce their information handling policies. When users send an email or create a new document, Titus leverages its machine learning technologies to automatically apply the appropriate classification based on organizational data security policies.

Titus' machine learning tools can evaluate the content and context of emails and documents, identify common document categories, and automatically apply or suggest increasingly accurate data classification. In many industries, certain document types are used again and again. For example, organizations in the financial sector create bank statements on a regular basis. In manufacturing, supply inventory spreadsheets are ubiquitous. Machine learning can understand the similarities between documents and then accurately apply automatic classifications.

The Titus Patrol feature keeps tabs on users' Downloads folder and scans files for sensitive content, classifying documents according to security policies. For example, if a user downloads a spreadsheet from Salesforce.com, Patrol would scan the spreadsheet, embed persistent metadata, and give it an appropriate classification immediately. Based on preconfigured policy requirements, Titus can also automatically add watermarks and any required information or category markings into the header and footer of a document.

All classifications are reflected in file names even when the file is closed, giving users an easy way to see whether a document contains sensitive information before they open it during a presentation or attach it to an email.

Share data confidently. Keeping track of the subtleties and layers of sensitive data created on a daily basis is no easy task for an individual user working in a home office. And employees working from home cannot easily turn to a coworker and ask questions about classification categories and information-sharing policies. Titus Config for Remote Work empowers users to share information confidently, providing numerous checks and balances that ensure data is protected and shared appropriately.

- **Reciept checking.** Titus Config for Remote Work keeps an eye out for information being shared with the wrong parties. Integrating with multiple browsers and email clients, Titus sends an alert to users if sensitive internal-only information is addressed to external recipients. Other guardrails can be set as well, including masking of names and contact information in the email CC: line.

- **Third-party domain blocking.** You can restrict or prohibit certain categories of documents from being sent externally or from being sent to specific domains. IT administrators have the option of adding an unlimited number of blocked domains to the list over time.

- **Email encryption.** Certain categories of documents attached in an email trigger data encryption automatically.

- **Data loss prevention.** Titus Config for Remote Work integrates with data loss prevention (DLP) technologies to alert users attempting to email or upload sensitive content to the cloud.

- **Sensitive data redaction.** Names, addresses, credit card numbers, social security numbers, and other personal details are redacted when emailed, uploaded to the cloud, or shared during video conferencing calls. If a user attempts to share a restricted file during a Zoom session, for example, the entire file will appear blacked out on screen. Default redaction blacks out an entire string of sensitive data, but you can create custom controls, which use smart regex to fine tune redaction parameters, such as blacking out all but the last four digits in a credit card number.
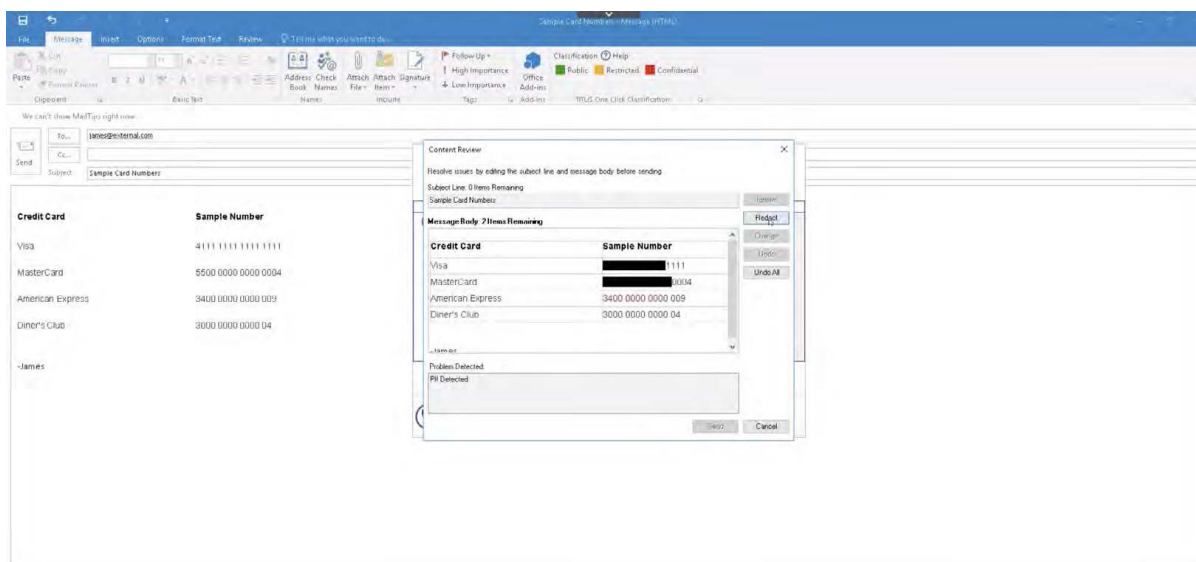
Titus allows you to set customized redaction parameters, such as blacking out all but the last four digits in a credit card number.

Produce valuable reports. Titus Config for Remote Work features an easy-to-use and flexible reporting feature that allows IT administrators to conduct remote worker usage audits and provide dashboard reports to business stakeholders. Reports can be generated from the Titus administrative console and distributed automatically to key stakeholders.

Easy, Accurate, Secure

Titus Config for Remote Work makes it simple for people working from home or otherwise outside of the office to accurately classify sensitive data and follow information handling policies on their own. Users are empowered to confidently and securely share information for increased collaboration and greater productivity, and IT admins and business leaders can rest assured that their critical data remains protected no matter where or how it travels.

titus
by HelpSystems

www.titus.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.