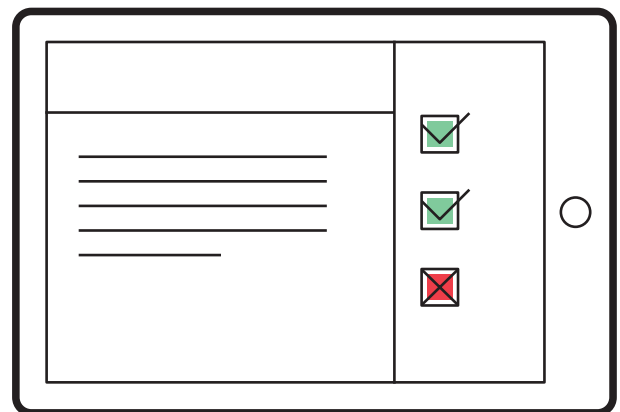


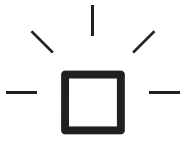


Secure Messaging™ for Government

Governments are among the fastest adopters of secure messaging.

Government agencies that adopt secure messaging are able to build better relationships with the public, increase internal efficiencies and establish a reputation of trust.





Secure Messaging Overview

Why Get Secure Messaging?

With increasing pressure to safeguard citizen data in an environment of growing regulatory oversight and increased information security risks, government agencies are among the fastest adopters of secure messaging and email encryption.

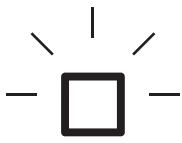
Yet governments worldwide are discovering that secure messaging encompasses far more than just email content protection. Secure messaging is becoming a core information management and communications tool that enables data loss prevention, large file transfer and secure mobile messaging.

Governments that adopt secure messaging are able to build better relationships with the public, increase internal efficiencies, save money and establish a reputation of trust.

Secure Messaging Overview

Secure Messaging is far more than traditional encryption. It's an information management tool that enables government agencies to easily protect and control access to their email even after content has left the outbox. In this age of heightened awareness of data security issues, Secure Messaging is a critical tool for government agencies looking to communicate more efficiently and effectively with their citizens and better serve their needs.

Secure Messaging is a cost-effective, cloud-based secure communications platform that's easy to use and quickly integrates into existing email infrastructure using existing email addresses. Additionally, Secure Messaging seamlessly integrates into any third-party archiving system. Government agencies appreciate the ease-of-use and the intuitive interface of Secure Messaging, which ensure agency-wide adoption of the secure messaging tools.



Secure Messaging Key Features



Simplified Secure Communications Exchange

Secure Messaging enables government agencies to simply and securely send, receive and track email communications internally and externally with the public on any device, including smart phones and tablets.



Data Loss Prevention

Secure Messaging works with any existing data leak prevention engine and can offer “intelligent keyword scanning” of message content based on an agency’s security policies and industry regulations. Plus, with the ability to fully revoke sent messages, data is always protected.



Large File Transfer

Secure Messaging enables both the sender and receiver to easily, quickly and securely share large file attachments of up to 5GB in size through email without overloading inboxes.



Regulatory Compliance, Electronic Tracking and Discovery

Secure Messaging supports the full spectrum of information privacy and security regulations. For electronic tracking and discovery purposes, Secure Messaging ensures messages are verified and intact, including who received it and whether it was read, along with date and time stamps.



No Technical Expertise Needed

As a cloud-based solution, Secure Messaging has no hardware to install, deploys in minutes and requires no outside IT expertise to implement. Ciuses integrates rapidly into existing email infrastructure including Outlook, Office365, Gmail and other standard email platforms using existing email addresses.

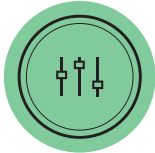


Fully Customized and Branded Secure Environment

Secure Messaging provides government agencies with a dedicated “slice” of the secure cloud that is fully customizable to match their security policies. The portal is also branded and encrypted for all customers and their existing email environment to create a seamless user experience.



Secure Messaging **Business Advantages**



Controlled communications

Secure Messaging's patented "Delivery Slip" provides real-time notifications so that employees can track when an email is received and read and control whether it can be replied to or forwarded. Employees can fully revoke a message after it has been sent and apply password protection for sensitive information.



Proof of receipt

Secure Messaging provides proof of delivery and prevents false claims of non-delivery.



Eases information exchange

Secure Messaging's secure and rapid large file transfer empowers government employees and the public to share any size of document securely using their regular email and email addresses without clogging up inboxes.



Protects against risks

With Secure Messaging's intelligent scanning feature, organizations can automatically prevent the accidental sending of sensitive information that should not be shared.



Cost effective with zero maintenance

As a cloud-based solution, Secure Messaging provides significant cost savings compared to in-house solutions, which are expensive to implement and maintain.



Data jurisdiction

Secure Messaging's cloud-based technology enables government agencies to choose in which country their data is hosted to avoid privacy risks imposed by international laws.



Reputation management

Secure Messaging enables government agencies to build a reputation of trust and security so that citizens feel confident sharing sensitive information electronically knowing their data is never at risk.



Secure mobile communications

Secure Messaging extends the secure messaging environment to smart phones and tablets to ensure information on every device is protected and controlled.



Integrates with any existing archiving system

Secure Messaging provides simple, automatic decryption into any existing archiving system to ensure seamless and full internal information management.