SECLORE

Seclore Data Protection Portal

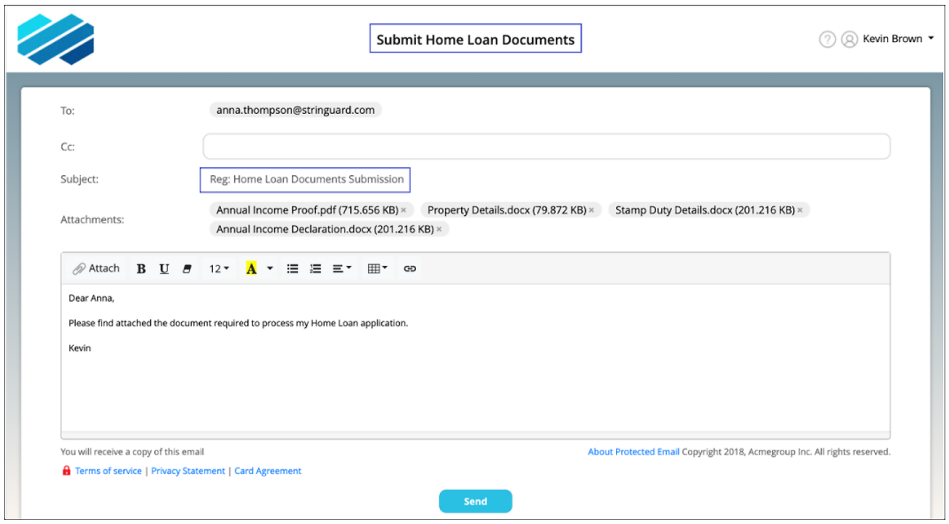
Organizations today are focused on protecting sensitive corporate data created within their borders and rightfully so. However, when customers, partners, and vendors send their confidential and sensitive data to an organization, the information is received unprotected. Because of this blind spot with regards to incoming data, sensitive documents remain unprotected within an organization as they are processed and shared internally by one or more departments.

The rise of tighter consumer regulations and fines, such as GDPR, CCPA, and DPA, are also placing additional pressure on organizations to secure all sensitive data. Organizations that receive sensitive data and fail to secure it risk exposing their company to compliance fines, insider threats, data breaches, reputational damage, and lost customer loyalty. Whether there are a few sensitive documents left unprotected or many, the liability for a company is the same.

Safeguarding Sensitive, Incoming Data

The Seclore Data Protection Portal automatically protects incoming sensitive data from customers, partners, and vendors by allowing administrators to configure predefined enforcement policies on incoming sensitive data received through the portal. When a customer, partner, or vendor shares sensitive information (home loan applications, health insurance claims, intellectual property) through the Seclore Data Protection Portal, persistent, granular usage controls are automatically attached to the documents before they reach employees' inbox.

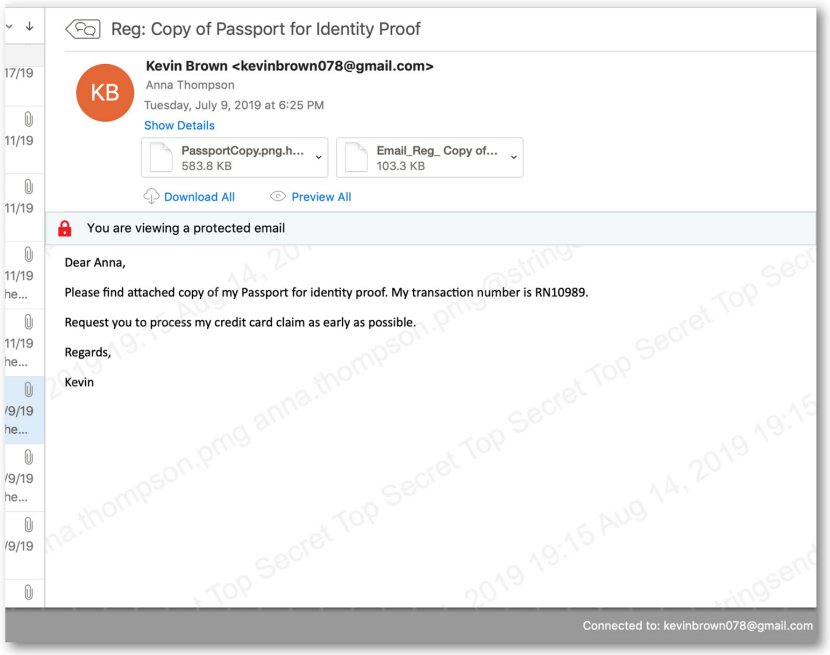
The Seclore Data Protection Portal assures organizations that sensitive information received through the portal from customers, partners, and vendors is secure and tracked throughout its lifecycle. Only preauthorized employees have access and usage rights (view, edit, print, share) to sensitive documents based on the predefined policies that are attached to the document. If an employee forwards the sensitive document to another employee, the granular usage controls travel with the document and can be modified or revoked at any time.



The customer attaches their sensitive documents to the user interface in the Seclore Data Protection Portal.

Simplifying the Protection of Incoming Data

Customers, partners, and vendors can easily utilize the Seclore Data Protection Portal once they validate their identity from their desktop or mobile device. Upon approval to access the portal, the individual can attach their confidential documents. The Seclore Data Protection Portal automatically applies access and usage controls to the sensitive documents based on the recipients, context of the email and other pre-



Incoming sensitive data is protected with usage controls (view, edit, print, share) when the employee opens the attachments.

defined usage controls. Organizations can assure customers, partners, and vendors that the sensitive information they share will be continuously protected from misuse or loss.

Automate Protection through Email or Uploading of Documents

The Seclore Data Protection Portal can be configured to allow customers, partners, or vendors, to either email or upload sensitive documents through the portal. As sensitive documents are shared through the portal by email or uploading, the Seclore Data Protection Portal attaches the appropriate security policies to the document. When an employee accesses the protected document, persistent, granular usage controls apply to the document when in-transit, in-use, and at-rest.

Keeping Incoming Information Secure

By automatically attaching security policies to incoming sensitive data from customers, partners, and vendors, organizations are reducing their risk of compliance violations and increasing trust with their constituencies. The Seclore Data Protection not only ensures an organization's collection of sensitive data is protected when in their possession but also makes secure collaboration is hassle-free.

End-user clicks a link to the user interface in the portal and attaches their documents

Data Protection Portal tags incoming data that is sensitive with an X-Header to add protection

Seclore's Email Auto-Protector reads the X-Header and attaches usage controls to the incoming data

Internal recipient receives the attachments with granular usage controls and tracking

Seclore Data Protection Portal automatically protects sensitive information shared through the portal with persistent, granular usage controls before reaching employees' inboxes.

SECLORE