A Seclore Whitepaper

SECLORE

Compliance with RBI Guidelines, Information Technology Act and PCI-DSS

Seclore's ERM and Data Classification

The Two Towers

CxOs of banks are losing sleep over the twin wake-up calls of outsourcing and compliance. Aspects relating to IT services outsourcing are now mandatory for banks to incorporate as part of their outsourcing policy as per RBI guidelines dated 29.04.2011, which also contain strict recommendations on the role of The Board and senior management of the bank.

Indian banks these days are stepping up war efforts to cope with the twin challenges of outsourcing and compliance. While issues on data sharing with third parties have kept IT, departments busy for quite some time, they also find their hands full with all sorts of regulatory and legal obligations – RBI Guidelines, the IT Act (2000) and subsequent amendments, Payment Card Industry : Data Security Standards (PCI-DSS) – the lot.

At first sight, many of these challenges – while sounding like common sense in theory - may seem paradoxical in practice. For example, the 2011 amendment of the IT Act (2000) stipulates that a bank or any person on its behalf (i.e. printing vendors, calling vendors etc.) shall not retain confidential information for "longer than is required". This stipulation - that parties should destroy all related assets once the relationship is terminated or after they is no longer needed - makes a token appearance in every single contract in the world. However, paper agreements are hardly enough to ensure that confidential data is destroyed in a timely manner. Or indeed - that the relationship between the bank and the service provider complies with the IT Act or the RBI Guidelines.

However, a bank can't just stop sharing important data with its vendors and service providers. After all, almost all banks in India have a well-established outsourcing and operational methodology – which in turn is a central pillar of their overall business strategy.

For many, this seems like a strange proposition. What other controlling mechanism can banks use to control their corporate assets and customer information lying with third parties? There is quite literally nothing that would stop a vendor from "accidentally" losing his laptop at an airport lobby. There's nothing that could stop someone from hacking an obscure printing vendor's site and siphoning off all that is required to start printing fake chequebooks. A bank's vendor can hang sensitive customer information out to dry, and there is nothing that a bank today can do to stop it. Since auditing cannot be considered an adequate control mechanism by itself – there is a need for a systemic solution that lets banks outsource their data – without being at the mercy of a piece of paper with a signature.

Borderless Security

How to Stop Being at the Mercy of Your Vendors' Environments

This problem is a circle that banks all over the country are desperately trying to square. For many, this seems like a strange proposition: how can I still control documents – ask IT chiefs – after they have left my premises? Despite having all their ducks lined up – Next- Generation Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Data Loss Prevention (DLP) systems etc. – a vendor can still misuse a bank's confidential information – accidentally or maliciously - and what a bank can really do to stop it is… exactly nothing.

Unless of course, you count a signature on a piece of paper as sufficient security.

Enter Enterprise Rights Management (ERM) – the only technology available today that allows organizations to secure their confidential information wherever it travels. This has the additional benefit of ensuring automatic compliance with regulatory and legal frameworks such as the RBI Guidelines (Gopalakrishna Report), the IT Act (2000) and subsequent amendments, and the PCI-DSS.

Seclore's ERM mapping with RBI Guidelines

The recommendations of the relevant RBI guidelines – on issues ranging from Information Security to Customer Awareness programs – prepared by the Working Group on information security, electronic banking, technology risk management, and cyber frauds, under the chairmanship of Shri G. Gopalakrishna, Executive Director, RBI - was circulated to all Scheduled Commercial Banks (excluding RRBs) for implementation on 29th April 2011.

The guidelines not only make it very clear that IT governance is an essential pillar of corporate governance – but also that RBI expects Indian banks to treat it that way. Enterprise Rights Management (ERM) has the potential to enable banks to comply with most – if not all – stipulations related to Information Security and Outsourcing. The following table lists specific cases (with page nos.) of the RBI Guidelines where Seclore's ERM directly enable compliance – and help mitigate the risk of data leakage and unauthorized data access.

Actual Guidelines	How Seclore can help
Data Classification: *"Information assets have varying degrees of sensitivity and criticality in meeting business objectives. By assigning classes or levels of sensitivity and criticality to information resources and establishing specific security rules/requirements for each class, it is possible to define the level of access controls that should be applied to each information asset.* *Classification of information reduces the risk and cost of over- or under- protecting information resources in aligning security with business objectives since it helps to build and maintain a consistent and uniform perspective of the security requirements for information assets throughout the organization. ISO 27001 standards require the inventorying of information assets and the classification, handling and labeling of information in accordance with preset guidelines."* **(page 17)**	Seclore's Data Classification assigns classifications to documents according to their sensitivity levels. Proper and appropriate classification is the first step towards adequate protection and access control. Seclore enables users to manually classify documents themselves on their computers. On the other hand, organizations can also choose to enforce document classification on users, who will be forced to select a classification for the document as soon as they attempt to close it. Moreover, Seclore's ERM protection for a document – along with classification - can either be enforced on the user (the file won't save and close until the user classifies the document) or made optional (the user can choose not to classify) depending on company policies. This flexibly to set (and enforce whenever necessary) classification policies enables banks to comply with this guideline without being at the mercy of employees' prior mental frameworks and forgetfulness. This decreases dependency on user actions and the possibility of human error – not to mention eliminating the additional training and IT overhead.
Data Security: *"A data security theory seeks to establish uniform risk-based requirements for the protection of data elements. To ensure that the protection is uniform within and outside of the institution, tools such as data classifications and protection profiles can be used."* **(page 29)**	Documents protected by Seclore's ERM remain protected wherever they travel. This ensures that documents contain the same level of security regardless of where and to whom they are shared – even on vendors' computers.

Seclore helps organizations quickly implement a Data Classification policy.

The protection provided by Seclore will persist even after these documents are sent outside the banks' internal networks, thus meeting the requirements specified in the RBI Guidelines, PCI-DSS and the IT Act.

Seclore's ERM is the ideal tool to comply with RBI Guidelines and to ensure uniform protection of data within and outside the bank.

Actual Guidelines	How Seclore can help
Data Classification: *"Management should establish access controls to limit access to media, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities. More sensitive information such as system documentation, application source code, and production transaction data should have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). Furthermore, policies should minimize the distribution of sensitive information, including printouts that contain the information. Periodically, the security staff, audit staff, and data owners should review authorization levels and distribution lists to ensure they remain appropriate and current."* **(page 30)**	Access controls are applied to documents themselves and not to the medium (such as in the case of shared network folders), thus reducing the burden of limiting access to physical media such as USB drives – and also reducing the subsequent liability that ensues as a result of not doing so. Every Seclore protected document is encrypted using military-grade encryption. The cryptographic keys are stored in the Seclore's database and do not travel with the encrypted document itself. Once a document is protected, it becomes absolutely tamperproof and its integrity is maintained wherever it travels. Users can be restricted from printing the document, but may be allowed to view it on a need-to-know basis. Complete audit logs of all permission lists and file activities are available via a browser-based console and are updated in real time.
Data Security: "Banks should encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination." **(page 30)**	Seclore's ERM uses multiple layers of militarygrade encryption to encrypt documents. A unique key is randomly generated for every document. The keys are stored in the central database and never travel with the document itself.
DLP: *"Concerns over the need to better control and protect sensitive information have given rise to a new set of solutions aimed at increasing an enterprise's ability to protect its information assets. These solutions vary in their capabilities and methodologies, but collectively they have been placed in a category known as data leak prevention (DLP). It provides a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework."* **(page 30)**	Seclore's ERM integrates with all major DLP solutions, including Symantec DLP, Websense DLP, McAfee DLP, GTB DLP, and MyDLP. ERM protection can be applied to data at rest, data in motion, and data in use based on violations of DLP policies or the triggering of DLP rules. ERM policies can automatically (without any user intervention) be applied to documents identified or discovered by DLP agents and crawlers based on the file content. This protection then persists with the document even after the file goes beyond the DLP's control perimeter, such as to vendors and partners. For example, an ERM policy can be applied to a document containing sensitive information if a user attempts to copy it to a thumb drive. Another example can be where an Email Gateway can be configured to not generate standard automated alerts when documents are sent with Seclore-protected

DLP and ERM are complementary technologies. Information leakage risks can be minimized by integrating Seclore's ERM with DLP solutions.

Seclore's ERM already has existing integrations with most major DLP products available today.

	Actual Guidelines	How Seclore can help
		attachments or even in the direct case of Seclore-protected emails. This is particularly useful when the organization's DLP implementation is in monitoring-only mode, and senior managers' inboxes are flooded with alerts. Hence, the capability and scope of DLP protection can be significantly enhanced by using it in conjunction with ERM.
Banks can share data with outsourced vendors and still continue to have peace of mind since the Seclore protected data shall remain safe and secure even at vendor locations.	**Information Security and Critical service providers / vendors:** *"The lack of controls and/or weakness in their design, operation or effectiveness can lead to consequences like loss of information confidentiality and privacy, systems not being available for use when needed, unauthorized access and changes to systems, applications or data, changes to systems, applications or data occurring that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system unavailability, loss of system resources and/or information assets and increased costs incurred by the enterprise as a result of any of the above."* **(page 38/39)**	Seclore protected documents always remain in the document owner's control – even after they are shared or distributed. Hence, even if the document is lost or lands in unauthorized hands (e.g. if the laptop or the USB drive containing the data is misplaced or stolen), unauthorized parties will not be able to open it at all.
Data shared with vendors providing services on Public Cloud platforms can also be safe if secured by Seclore's ERM.	**Cloud Computing:** *"The lack of controls and/or weakness in their design, operation or effectiveness can lead to consequences like loss of information confidentiality and privacy, systems not being available for use when needed, unauthorized access and changes to systems, applications or data, changes to systems, applications or data occurring that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system unavailability, loss of system resources and/or information assets and increased costs incurred by the enterprise as a result of any of the above."* **(page 57)**	Since Seclore's ERM protection is applied on the file itself and not on the medium or storage, documents always stay protected – in transit and in the cloud. Seclore's protection is independent of the file's storage mechanism or transmission medium. Hence, even if the cloud service provider suffers from a data breach, the data still remains secure and cannot be accessed by unauthorized parties. Seclore's ERM has the ability to integrate with an organization's existing authentication and authorization mechanism – including an Identity and Access Management system, a federated identity management system and/or a simple SAML-based SSO server on the cloud. Hence, the same level of authentication-related compliance can be maintained for Seclore's ERM as for other IT solutions, including the Windows Active Directory. All activities performed on protected files by authenticated users – whether inside or outside the enterprise network - are centrally logged in the system.

Actual Guidelines	How Seclore can help
Material Outsourcing: *"Nature and extent of data sharing involved. For e.g., where outsourcing involves sharing of customer data, the engagement may be 'material'... Impact on data privacy and security. For e.g., whether access to customer data has to be extended to staff of the service provider"* *"Whether the bank has adequate flexibility to switch service providers, so that the risk of being attached to a single service provider is adequately mitigated, and the aggregate exposure to a single service provider."* **(page 76/77)**	Seclore's ERM can assign access rights to named users on each protected document. Hence, specific users in the service provider's organization can be identified and information shared on a need-to-know basis. This reduces the risk of data leakage and mitigates against the possibility of unauthorized data access. Seclore's ERM protected files can be expired remotely and made inaccessible on demand (in real-time) or after a certain time period has elapsed. Any attempts to access the files after the specified expiry date are also logged. Hence, this reduces the compulsion for banks to be tied down and be at the mercy of one service provider or vendor just because of previously shared customer data – thus offering unprecedented flexibility to switch providers at any time.
"Control Environment offered by the Service Provider: • *Control considerations for handling of customer information and personally identifiable information* • *Data classification and controls for handling data."* **(page 82)**	Since Seclore's ERM protection is completely independent of storage mechanism and transmission medium, there is no dependency on the environment – cloudy or otherwise – offered by the service provider. A Seclore protected document will always carry the same (and also the maximum possible) level of security – whether it is shared via a VPN (Virtual Private Network) or uploaded on an FTP server. Hence, in theory as well as in practice, Seclore's ERM protection is equally effective in any environment.
Confidentiality and Security: *"Public confidence is a cornerstone in the stability and reputability of a bank. Banks should be proactive to identify and specify the minimum security baselines to be adhered to by the service providers to ensure confidentiality and security of data. This is particularly applicable where third party service providers have access to personally identifiable information and critical customer data. An institution may discuss and agree on the instances where customer data shall be accessed and the user groups who will have access to the same. Access to a Bank's data should be strictly on a need to know basis."***(page 83)**	Seclore offers full training, documentation, consulting, and product support for successful deployment and usage of Seclore's ERM solution. This includes a detailed and comprehensive Data Flow Analysis (DFA) of information to and from vendors and service providers, as well as a detailed analysis of internal business processes. The Seclore's ERM solution can be tailored around a bank's existing business process workflows – rather than the other way around.

Seclore's ERM reduces the compulsion for banks to be tied down and be at the mercy of one service provider or vendor just because of previously shared customer data – thus offering unprecedented flexibility to switch providers at any time.

Data shared with third parties can be, post-facto and remotely, made non-accessible by the sender. Thus, in case of a change in the business relationship (including parting with the vendor), the security risk on the vendor side reduces drastically.

By implementing Seclore's ERM, banks can literally comply with the stipulations and get protection in case of lawsuits and legal complications.

Seclore's ERM and the IT Act

The IT Act (2000) signaled the coming of age of the Indian legal framework to a traditionally ignored area. It was the first step towards providing legal acknowledgment and recognition to the exchange of electronic information and electronic commerce. Major amendments were weaved in 2008 and 2011 in the form of the Information Technology Amendment Act or ITAA – which provided increased focus on Information Security. It was no longer enough to just secure a network, datacenters, and databases. It is information that really drives an organization – and it is this information that organizations are now legally obliged to protect.

Customers can now sue banks under the IT Act for data leakage incidents or data theft, even if the actual incident or theft emanates from a vendor or partner.

For enterprises, the IT Act and the subsequent amendments and gazette notifications have resulted in increased liability for lapses in data privacy and data security. Customers can now sue banks under the IT Act for data leakage incidents or data theft, even if the actual incident or theft emanates from a vendor or partner.

Seclore's ERM usage enables an enterprise to not only ensure the privacy and security of its sensitive data, but also enables automatic compliance with the IT Act. It places unprecedented power in the hands of a bank – hands that they would otherwise have full in complying with the Act – to not only mitigate against the risk of data theft and leakage but also virtually eliminate the risk of litigation and legal action.

Seclore's ERM Mapping with the IT Act (2000) and Amendments

The following table lists the actual section/clause of the IT Act and its amendments and how Seclore's ERM ensures direct compliance with each of them.

The security of ECM and DMS systems such as SharePoint and FileNet can be extended to locations beyond their jurisdiction – by applying a security layer to the documents themselves. Hence, the security offered by such systems can be extended to wherever the actual documents are shared or distributed.

Stipulations	How Seclore can address this statutory requirement
"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network… (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (I) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, he shall be liable to pay damages by way of compensation to the person so affected." **(Section 43)**	Seclore's Enterprise Rights Management can integrate with DMSs (Document Management Systems) such as Sharepoint, FileNet, Documentum, Omnidocs etc., data repository, or transactional/ERP systems. Any information extracted from such systems (e.g. a report in Excel form) can be automatically protected with Seclore's ERM. Hence, the security offered by such systems can be extended to wherever the information is shared or distributed. Seclore's ERM enables information owners to restrict users from altering information. Users may have permissions to view the content, but not to edit it in any way. All unauthorized (and unsuccessful) attempts to edit and save the content are logged against the identity of the individual user.

Stipulations	How Seclore can address this statutory requirement
	Hence, proper usage of Seclore's ERM can help banks mitigate the risk that can ensue due to alteration of customer records and other confidential data by people acting on its behalf - employees and vendors. Even unauthorized attempts to edit information are logged, along with other forensic details such as the user's name, the activity date and time, requesting IP address, machine name etc. – thus making auditing easier and more flexible.
"A body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force." **(Section 87 read with Section 43A - Gazette notification dated 11.04.2011)**	Seclore-protected files can be expired remotely and made inaccessible on demand (in real-time) or automatically after a certain date or time period. Any attempt to access the files after the specified expiry date is also logged. Hence, banks can avoid the risk of litigation by ensuring that its employees or vendors/partners do not hold sensitive personal data for longer than is required.
"6. (4). Disclosure of Information: The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further…" **(Section 87 read with Section 43A - Gazette notification dated 11.04.2011)**	With Seclore's ERM solution, banks can ensure that information is accessible only to authorized users. Unauthorized users – even if they manage to get hold of protected documents – will not be able to access the information in any way. Hence, banks can avoid the risk of litigation by ensuring that no-one except designated and trusted third-party collaborators can access sensitive personal data.
"7. Transfer of information: A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules." **(Section 87 read with Section 43A - Gazette notification dated 11.04.2011)**	Information protected by Seclore's ERM possesses the same level of protection regardless of where it travels – there is no dependency on the vendor environment. Hence, the same level of data protection can be maintained anywhere the information is shared or distributed.

Seclore also helps comply with stipulations related to limiting vendors from retaining customers' personal data and information after processing.

Information can be sent out with an expiry date – so that they automatically expire after a certain time and date. Documents can be expired remotely in realtime from anywhere in the world.

The ABC of ERM and PCI-DSS

Seclore helps banks directly comply with PCIDSS, particularly with respect to cardrelated data shared with third parties.

Hacking seems to be the buzzword in the industry these days. Today's news is atwitter with apocalyptic news about how no company is secure, or about how there are only two types of organizations in the world – one that has been hacked, and the other that has been hacked but doesn't know it yet. FBI Director Robert Mueller testified last year that hacking could soon replace terrorism as the FBI's primary concern.

Eddie Schwartz, the Chief Security Officer at RSA, recently remarked that "Hackers view India as a target. It's got a fast-moving economy, a fast-moving IT infrastructure". The word "fast-moving" can almost be interpreted as an euphemism for nascent and emerging.

Eddie Schwartz, the Chief Security Officer at RSA, recently remarked that "Hackers view India as a target. It's got a fast-moving economy, a fastmoving IT infrastructure". The word "fast-moving" can almost be interpreted as an euphemism for nascent and emerging.

Nowhere is this more important than the banking and financial services industry. Unprotected data lying around in unsecured vendor environments (and in transit) is low hanging fruit for both hackers as well as disgruntled employees. The Payment Card Industry - Data Security Standard (PCI-DSS) is a set of robust classification and security standards that seek to enhance the handling of payment card-related information. It must be implemented by all entities that process, store or transmit cardholder data. Compliance with PCI-DSS is an essential component of the overall security framework of any bank. The Reserve Bank of India has made it mandatory for all Indian banks to implement PCI-DSS.

Seclore's ERM enables direct and automatic compliance with PCI-DSS. The following table lists details about the actual clauses that are ticked off when an organization is actively using Seclore's ERM. These are explicitly applicable for card-related data shared with third parties.

PCI-DSS requirement	How Seclore can address the requirement
"Implement a data retention and disposal policy that includes: *— Processes for secure deletion of data when no longer needed."* **(Clause 3.1.1)**	Seclore's ERM solution allows a document owner to remotely expire information at any time from any location. An owner can also set expiry dates to information before sending it – both in terms of a specific date and time or a time period (number of days). After the specified time period, the information will not be accessible. This expiry can also be made user-specific. For example, the same document can be made inaccessible to one user while another may continue to access it.
"Do not store sensitive authentication data after authorization (even if encrypted). Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely." **(Clause 3.2)**	No authentication data is stored by the Seclore system locally[1]. Seclore's ERM solution authenticates users from via a designated and configured user repository, such as the Windows Active Directory.

Data retention and purging can be driven by Seclore's ERM instead of manual processes and oversight.

[1] *Except when the user has offline access permissions on the file.*

For unstructured data (i.e. files) shared with third parties, the encryption used by Seclore helps banks comply with the guidelines.

PCI-DSS requirement	How Seclore can address the requirement
"Render PAN (Card number) unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: *— One-way hashes based on strong cryptography (hash must be of the entire PAN)* *— Truncation (hashing cannot be used to replace the truncated segment of PAN)* *— Index tokens and pads (pads must be securely stored)* *— Strong cryptography with associated key-management processes and procedures* *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN."* **(Clause 3.4)**	Seclore uses military-grade encryption in a multi-layered fashion with multiple dimensions and parameters involved. The decryption keys for every document do not travel with the document itself and are never stored on users' computers[2].
"Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are: *a) The Internet,* *b) Wireless technologies,* *c) Global System for Mobile communications (GSM), and* *d) General Packet Radio Service (GPRS)."* **(Clause 4.1)**	In accordance with PCI-DSS, banks need to implement strong cryptography and security protocols for payment transaction systems. This needs to be ensured at all the hops related to card transactions. However, there are multiple vendors that receive cardholder data in unstructured form (i.e. in files) – and this data also needs to be delivered by the bank to the vendor in a secured manner. Securing the medium instead of the message may leave the information open to man-in-the-middle and similar attacks. In the context of cardholder-data file sharing with third parties, Seclore's ERM encrypts the files themselves with no dependence on the medium. Thus, encrypting the transmission or storage medium can be avoided. Seclore's protection is independent of both the transmission and storage mediums. Hence, there is absolutely no risk in sending the file over a public network. In fact, a Seclore protected file remains as secure when travelling over a public network as it is when inside a VPN (Virtual Private Network) tunnel.

[2] *Except in case of offline access permissions being provided to the recipient, where the key is stored on the local system (in encrypted form) to enable offline access.*

PCI-DSS requirement	How Seclore can address the requirement
"Limit access to system components and cardholder data to only those individuals whose job requires such access." **(Clause 7.1)**	Unauthorized users cannot access Seclore protected information. All access attempts are centrally logged and audit reports can be pulled from a central console.
"Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed." **(Clause 7.2)**	Users cannot access Seclore protected data unless they are specifically allowed to do so by the information owner. Permission is always maintained on a need-to-know basis and denial to information is the default.
"Implement automated audit trails for all system components to reconstruct the following events: — *All individual accesses to cardholder data* — *All actions taken by any individual with* — *root or administrative privileges* — *Access to all audit trails Invalid logical access attempts."* **(Clause 10.2)**	A detailed audit trail is available for activities performed on Seclore protected files. Both authorized and unauthorized attempts to access the document (from any location) are automatically logged, including forensic details such as host name, requesting IP, etc. Automated alerts and business intelligence (BI) reports can be generated by easy integration with SIEM and BI tools. Configuration and management actions taken by users with root or administrative privileges are also logged in the system. Detailed audit trail reports are available for various scenarios and filtering criteria.

Seclore's ERM is based on a strong access control philosophy.

An automated audit trail containing details of access to Seclore-protected files is available.

Protect Your Information – Anytime, Anywhere

With customers including Axis Bank, HDFC Bank, and Kotak Mahindra Bank in India, and banks such as Sberbank of Russia abroad – Seclore's ERM has been proven again and again to enable organizations to:-

1. protect confidential information
2. eliminate data leakage and data theft, especially while outsourcing business operations
3. comply with the relevant guidelines and regulatory compliance obligations

The day is not far when banks face legal action and fines/penalties under the IT Act for a data breach at a vendor location (where the bank has no control) or by leakage of confidential information by employees. With Seclore's ERM, Indian banks can now ensure not just the safety and security of their information, but also eliminate the risks associated with external collaboration – and comply with all the relevant guidelines in the process.

About Seclore

Seclore offers the market's first fully browser-based data-centric security solution, which enables organizations to control the usage of files wherever they go, both within and outside of the organization's boundaries. The ability to remotely enforce and audit who can view, edit, copy, screen share, and redistribute files empowers organizations to embrace mobility, file-sharing, and external collaboration with confidence. With over 6000 companies in 29 countries using Seclore to protect 10 petabytes of data, Seclore is helping organizations achieve their data security, governance, and compliance objectives.

Learn how easy it now is to keep your most sensitive data safe, and compliant.
Contact us at: info@seclore.com or CALL 1-844-4-SECLORE.

USA – West Coast
157 S. Murphy Avenue
Sunnyvale, CA 94086
1-844-473-2567

USA – East Coast
420 Lexington Avenue
Suite 300,
Graybar Building
New York City
NY 10170

India
Excom House Ground Floor
Plot No. 7 & 8,
Off. Saki Vihar Road
Sakinaka, Mumbai
400 072
+91 22 6130 4200
+91 22 6143 4800

Gurugram
+91 124 475 0600

Bengaluru
+91 080 46586900

Singapore
Seclore Asia Pte. Ltd.
#08 -01
80, Robinson Road
Singapore – 068898
+65 8292 1930
+65 9180 2700

Europe
United Kingdom
Suite 4B, Linwood Point
Paisley, PA1 2FB
+44 141 433 7902

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+97155-990-1570
+9714-440-1348

Saudi Arabia
5th Floor, Altamyoz Tower
Olaya Street
P.O. Box. 8374
Riyadh 11482
+966-11-212-1346
+966-504-339-765

SECLORE