A Seclore Whitepaper

SECLORE

Complying with UAE Cabinet Resolution No. 21 of 2013 Regarding Information Security Regulation

Seclore's ERM and Data Classification

Mohammed issues Cabinet decision on IT security regulations

Friday, December 13, 2013

UAE Vice President, Prime Minister and Ruler of Dubai His Highness Sheikh Mohammed bin Rashid Al Maktoum

UAE Vice President, Prime Minister and Ruler of Dubai His Highness Sheikh Mohammed bin Rashid Al Maktoum has issued Cabinet Decision No. 21 of 2013 on Information Technology (IT) security regulations at federal government entities. Dubai's Information Security Committee (ISC) is coordinating with various government agencies to implement the Information Security Regulation (ISR), aimed at managing the information security environment in Dubai's public sector.

Seclore's Enterprise Rights Management is a simple yet effective way to not only secure your critical data from falling into the wrong hands, but also complying with the Resolution.

This proven technology has gained wide acceptance all over the world, including in the Middle East. Seclore's ERM is being used by eminent organizations such as AL-ELM (Riyadh), Crown Price Court (Abu Dhabi), National Bureau of Statistics (UAE), ASRY (Arab Shipbuilding and Repair Yard, Bahrain), ADMA (Adnoc Group), and Panasonic (UAE); Daimler, Linde Engineering, GE Capital; and financial organizations such as NSE (National Stock Exchange - India), HDFC Bank, ING Life, ICICI Lombard, ICICI Prudential, PNB MetLife, Reliance Capital, various insurance companies and many more.

This white paper discusses

- The UAE Cabinet Resolution No. 21 of 2013 on Information Security
- How to secure unstructured data - files, documents, and emails - from data theft and leakage
- How Seclore's ERM can help Federal Entities easily comply with the Resolution

The Real Information Assets: Files and Documents

Unstructured data – data stored in Word documents, Excel spreadsheets, PDF documents etc. – is extremely difficult to secure and control. It is also shockingly easy to leak or steal. Moreover, this data goes out to external collaborators (vendors, partners, auditors etc.) on a regular basis without any security or controls whatsoever.

According to research firm Gartner,

- Unstructured data represents as much as 80% of an organization's information assets[1]
- Its growth rate is also around the same, with the rate for structured data being about 40-60%[2]

Unstructured data exists inside digital documents such as Word files, Excel spreadsheets, PDF files, emails etc. Unlike data in data repositories or databases, this type of data does not conform to any specific data model or standard. It is free to travel wherever the user decides to send it – and it often travels with no restrictions whatsoever.

Structured data is typically stored inside a data repository or a database. Unstructured data, on the other hand, has no fixed storage mechanism. It can reside on a file server, a local laptop or desktop, a smartphone, a USB drive, a CD or DVD, and even on the cloud. It is surprisingly easy to share (or steal) unstructured data: anyone can send it to anyone else via email, a shared network folder, a thumb drive, a CD/DVD, a cloud storage service – the possibilities are endless. However, with great ease comes great risk. Since unstructured data is easy to share, it is also easy to leak or steal. Organizations thus incur great liability by allowing their employees to create, own, and distribute copies of such data – copies that might easy land up in the wrong hands. Although it is imperative for organizations to allow business users to create and distribute data due to genuine business needs, in today's world, it has also become imperative to secure that data from unauthorized usage.

Governing Government Employees

There can be national security implications for the leakage of federal data.

This problem becomes more acute for organizations affiliated with the government Unstructured information in a government organization includes not just business critical and confidential data, but data that may be highly sensitive due to national security concerns. Moreover, it may be highly embarrassing for a federal government organization – and indeed the government itself – to find its top secret data being misused or stolen by rival governments or just auctioned on the market by a disgruntled employee. The sheer size of not just the unstructured data but the organization itself mandates the usage of an information-centric security solution - a solution that will protect your data wherever it travels.

UAE Cabinet Resolution No. 21 of 2013

Federal entities are now legally mandated to enforce Information Security policies with the passing into law of the UAE Cabinet Resolution No. 21 of 2013

Protecting these unstructured information sources has always been a high priority for federal and government-affiliated organizations in the UAE. However, Information Security has now become legally mandated and formalized with the passing into law of the unprecedented UAE Cabinet Resolution No. 21 of 2013. This Resolution provides a legal framework to information security and regulate the safety of confidential assets in federal institutions. It requires that IT departments take maximum precautions to protect their critical information and enforce strict security policies on the usage and movement of such information assets. The Resolution applies to "the ministries, public corporations, institutions and public bodies affiliated to the federal government". This includes ministries, such as the UAE Ministry of Economy, and other federal government departments and entities such as the UAE Central Bank.

[1]*Darin Stewart, Gartner. (2013). Big Content: The Unstructured Side of Big Data. [Online] Availablefrom:http://blogs.gartner.com/darin-stewart/2013/05/01/big-content-the-unstructured-side-of-big-data [Accessed: 17th February 2012]*

[2]*Gartner. (2011) IT Market Clock for Storage, 2011.*

In its own words[1], the Resolution aims at

1. Strengthening the concept of InfoSec at FEs (Federal Entities) and Users.
2. Identifying the standards of the optimal use of IAs (Information Assets).
3. Encouraging the effective application of electronic security (e-security) by enhancing it as a collective effort that requires the participation and support from all Users.
4. Ensuring that all Users are informed with their duties regarding the use of IAs.
5. Identifying measures that FEs shall follow to protect Users against illegal or malicious actions that may lead to damaging IAs.
6. Providing legal framework for FEs for ensuring the security of IAs.
7. Creating a safe environment in FEs for maintaining information by ensuring the confidentiality of information and network infrastructure and protecting it by preventing non-authorized access, editing, exchange, loss, leak, damage, malicious by any of means.
8. Addressing InfoSec-related risks, identifying potential risks and addressing them to ensure the continuity of workflow in FEs in case of exposing to any incident or attack.

Seclore ERM controls not just access to the data, but also its usage Seclore's protection secures the file even when it is on a vendor's or partner's laptop.

Non-compliance of this resolution may lead to criminal liability under UAE law, which in turn could lead to fines or even imprisonment. In addition, individual employees are already subject to internal disciplinary regulations and penalties of the federal authorities that they work for. Every federal employee is required to sign an acknowledgment and commitment of having understood and being committed to the guidelines. The resolution stipulates that "every User (who) violates the provisions of this Regulation shall be punished according to the disciplinary sanctions set forth in the human resources laws and regulations applied in the FE he/she works for".

How Seclore's ERM can help Seclore's ERM

Seclore's ERM[2] is a technology that enables information owners to secure their unstructured information and then control and monitor its usage. Protecting a document with ERM ensures that only the right people get access to it. And further – it ensures that those right people are able to do only right actions with the document (viewing, editing, printing etc.) at the right time and from the right location. ERM applies a security blanket around the document that persists with the file wherever it goes – even outside the organization to vendors, partners or other external collaborators.

ERM can easily plug into an organization's existing infrastructure and business process workflows. Seclore's ERM can be easily integrated with other IT solutions such as ECM, DMS, DLP, Email and Messaging, transactional systems etc.

Hence, ERM governs not just access to the data, but also its usage. For example, an authorized user may be allowed to read the contents of a document (say a PDF or Word file) but could be restricted from editing or printing it. ERM can also enable the file owner to control the document remotely. The owner may disable or expire the information at a time of his own choosing, or may send the document out with predefined time-based controls. For example, a tender can be sent out with an expiry date – after which it will be inaccessible. A bid document can be distributed with a specific accessibility time period - say the 10th to the 15th of next month. The document will start being accessible only from the 10th - and remain accessible only till the 15th.

[1]*Cabinet Resolution No. 21 of 2013 Regarding Information Security Regulation in the Federal Entities, The Cabinet, United Arab Emirates*

[2]*Also known as Enterprise Rights Management (E-DRM)*

Seclore's ERM enables direct and straight-forward compliance with UAE Cabinet Resolution No. 21 of 2013.

How Seclore's ERM maps with UAE Cabinet Resolution No.21 of 2013

Seclore's ERM usage can help an enterprise comply directly with most information security guidelines posed by the Resolution. Multiple features of Seclore's ERM solution enable an organization to not just secure their critical assets, but also successfully comply with the Resolution at the same time. The table below explains how.

Description/Actual Text	How Seclore can address this requirement
This article contains multiple points that requires federal entities to enforce a password policy for users "User shall make that he/she uses a secure and effective passwords and keeps it secure at all times. For creating a password, User shall commit to: a) The Password shall include capital and small latten letters such as (A-Z) (a-z), numbers and punctuation (>`_()*^%$#@!). b) The Password shall not be less than 8 characters (alphabets, numeric, or symbols). c) The Password shall not be personal information that might be easily guessed… …expiry date of Passwords which shall not be less than (60) days and User shall not use the same Password for more than once within (180) days and not more than (90) days and User shall not use the same Password for more than once within (180) days. The Password shall not be re-used within (6) rounds of changing…" **(Article 6: Rules for creating password)**	Seclore can be plugged into the existing Identity and Access Management systems of an enterprise (including the Active Directory), thus ensuring that the same passwords and password policies apply to ERM too. Moreover, Seclore's ERM comes inbuilt with a user repository that can be used to onboard external users. Password policies can be enforced on users that are part of this repository, including automatic password expiry and resetting.
Points 1 to 5 deal with the use of desktops and laptops and their probable loss or theft. **(Article 11: Controls of the use of desk computers and laptops)**	Seclore's ERM protection is independent of file location and storage. It persists with the file even when the storage media (in this case a laptop) is accessed by unauthorized users, who will not be able to access the file itself. Moreover, files can be locked by the file owner or an administrative user from any location. Hence, in the unfortunate case of a stolen laptop or device, Seclore-protected files can be expired remotely. This will ensure that the file will never open. These Seclore's ERM features severely reduce the risk associated with stolen laptops or mobile devices.

Description/Actual Text	How Seclore can address this requirement
"1. provide the greatest protection of the classified, sensitive and confidential information through the effective use of data encryption… *2. provide the appropriate encryption measures to any data sent via the network of other, and basic public communications networks…* *3. encrypt and protect confidential data transmitted via readable fixed storage media in the computer…* *For data encryption, user shall commit to …encrypt all existing sensitive and confidential data when storing or sending it"* **(Article 12: Encryption)**	Seclore has been cleared for – and is currently in use by – numerous military and government agencies across the world, including the APAC, EU, and the Middle East regions. Files remain encrypted and protected regardless of the storage mechanism (e.g. thumb drives and other storage media) and transmission medium (e.g. an unsecured network). Seclore uses military-grade encryption in a multi-layered fashion utilizing multiple dimensions and parameters. Custom and propriety encryption algorithms can also be plugged into Seclore's ERM. The cryptographic keys never travel with the file itself. All keys are stored in the central Seclore database and are always separated from the content. In general, the document content also never travels to the Seclore server or database - but is always encrypted in its original location.
"1. Levels of confidentiality of FE documents, papers and information and people who have the right to access to every level of confidentiality shall be determined as follows: a - Very confidential: shall be given to the information with a strategic importance to the Country and the Federal Entity, as it requires the highest levels of protection. The right to access such information shall be given only to a few numbers of competent users. b - Confidential: shall be used for information that may have detrimental effect on FE. The number of users which shall have the right to access this information shall be limited (e.g. a specific department or job title) c - Restricted: shall be used for the information that does not harm if it is circulated between various FE departments. d - Public: shall not be considered of the confidentiality levels and this level shall be used for information that can be accessed by public." **(Article 14: Levels of Confidentiality)**	Seclore's ERM allows an organization to classify documents based on customized and pre-determined access levels. Users can classify a file manually on their computers. This eliminates the risk of false positives that are generally encountered with other automated (content-aware) data classification solutions such as DLP. File classification can also be made mandatory for users (i.e. the file will not save and close until the user classifies it). ERM can also enable content-based classification with integration with DLP solutions. Seclore's ERM integrates with all major DLP products such as McAfee DLP, Symantec DLP, Websense DLP, GTB DLP, and MyDLP. Seclore also offers a stand-alone classification solution that can be used to classify files without applying any encryption or rightsbased protection. This classification can be read by other solutions (e.g. DLP) and appropriate DLP policies or rules can be triggered. For example, only files tagged "Public" would be allowed to be copied to any external storage media such as a thumb drive.

The resolution places an obligation on federal authorities to enforce classification of information assets by employees. This unprecedented approach is generally considered by experts to be more sophisticated and intricate than other legislation in the UAE.

"FEs shall be responsible for classifying the levels of confidentiality for its information correctly, selecting its storage media and the periodic review of this classification and defining User powers according to the classification in terms of access, editing, deletion, copying, sending or printing." **(Article 14: Levels of Confidentiality)**	All classifications in Seclore's ERM solution can be centrally controlled. Audit logs are available from a central console and audit reports can be extracted based on various criteria. These reports can also be structured to facilitate compliance reporting for frameworks such as ISO 27001, Sarbanes Oxley, GLBA, PCI DSS & HIPAA. Access to information can be restricted based on its classification. For example, printing a confidential document may be restricted altogether for all users. With DLP Integration, files classified as 'Public' would have no travel restrictions imposed on them and would be freely allowed to be copied or sent to an external location. To take another common example, the Email Gateway can be configured to ensure that all emails containing attachments classified as "Confidential" and above shall be blocked. Or – all emails containing "Restricted" attachments shall be allowed to go only to white-listed email addresses, and so on.
This article contains various points meant to restrict the usage of external storage media. **(Article 16: Controls of data storage)**	Seclore's ERM protection is applied persistently – it remains in effect everywhere the document travels and resides – even in external data storage media. Hence, the risk and liability associated with the usage of external media is severely reduced. Moreover, as specified above, there is absolutely no risk of unauthorized access to the Seclore protected information residing in the media (and laptops as well) if it is stolen or misplaced.
"I, the employee undersigned, hereby acknowledge that I have read and understood the Commitment and I shall be committed to it." **(Annex to the Cabinet Resolution No. 21 of 2013)**	Although NDAs and contracts are essential for liability and legal purposes, they are hardly a deterrent against accidental – or even malicious – date misuse or leakage. With Seclore's ERM, protection of information ensures that federal entities don't have to rely on a signature on a piece of paper to ensure that their data doesn't fall into the wrong hands.

Every federal employee is legally liable for noncomplaince of this Resolution. Every individual is required to sign an acknowledgment to this effect.

No More Data Theft

With customers in 29 countries, including multiple successful deployments in the Middle East – Seclore's ERM solution has been proven again and again to enable organizations to protect data, prevent unauthorized access, and facilitate compliance with government regulations. With information that remains protected both within the organization and after it has left the building, enterprises can sleep at night without worrying about disgruntled federal employees or their outsourcing vendor's lax security apparatus. In today's post-Wikileaks world, it has become shockingly common for individuals to leak even the most top-secret data. With Seclore's ERM, Federal Entities and other enterprises in the UAE can now easily prevent such leaks.

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 2000 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
691 S. Milpitas
Blvd.#217
Milpitas CA 95035
1-844-473-2567

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

India
Excom House Second 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

Singapore
Seclore Asia Pte. Ltd.
AXA Tower, 8 Shenton
Way
Level 34-01
Singapore – 068811
+65 8292 1930
+65 9180 2700

Europe
Seclore GmbH
Marie-Curie-Straße 8
D-79539 Lörrach
Germany
+49 151 1918 5673

UAE
Seclore Technologies FZ-LLC
Executive Office 14, DIC
Building 1 FirstSteps@DIC
Dubai Internet City, PO Box
73030, Dubai, UAE
+9714-440-1348
+97150-909-5650
+97155-792-3262

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

SECLORE