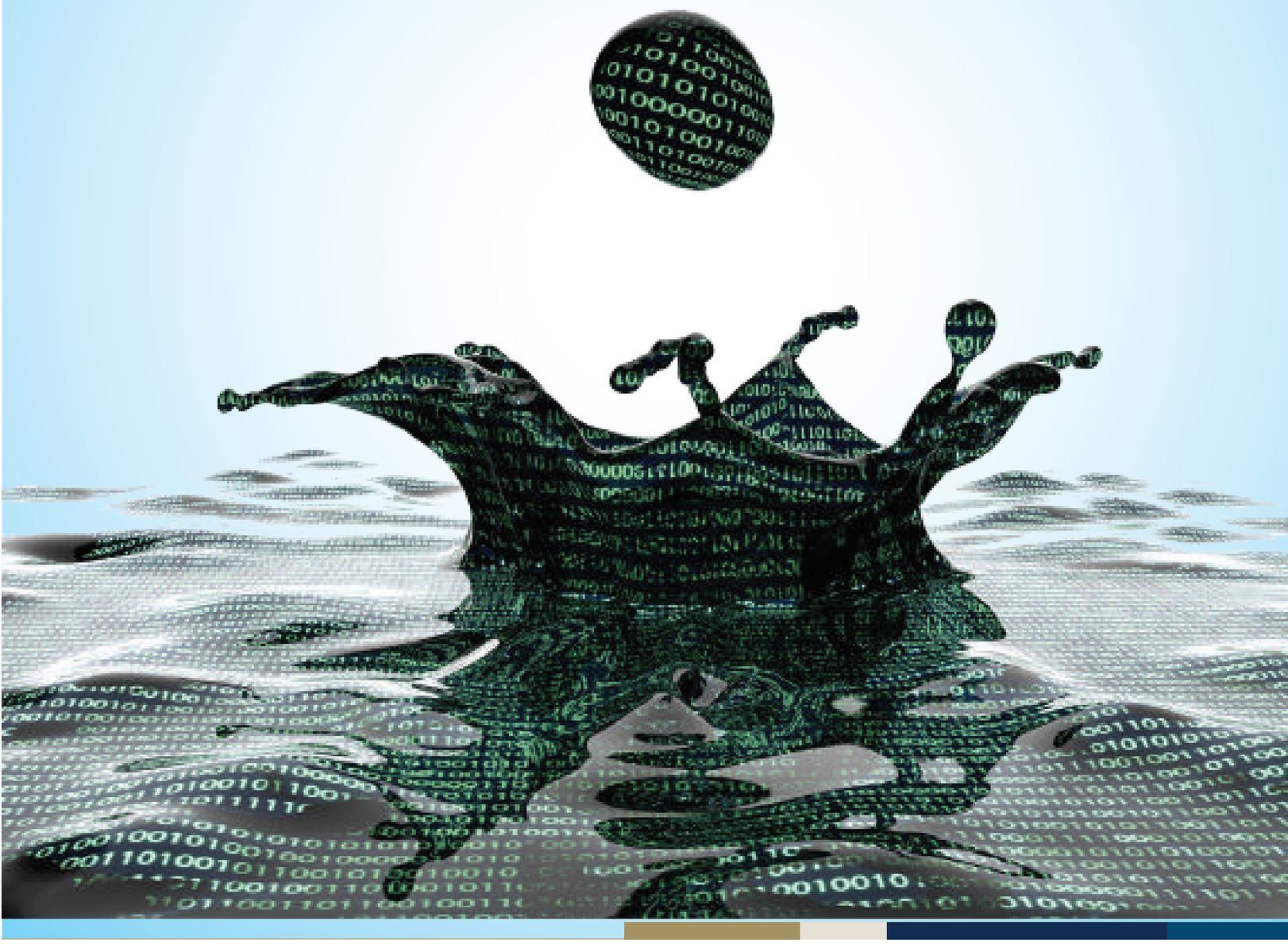
# A Guide to Information Security and Data Protection Laws in GCC Countries

2018-2019

STA



Our Offices: Abu Dhabi | ADGM (Abu Dhabi) | Bahrain | Delhi | Doha | Dubai | Fujairah | Lisbon | London | Luxembourg | Moscow | Ras Al Khaimah | Sharjah

# CONTENTS


1. What is Information Security?
   - 1.1. Confidentiality
   - 1.2. Integrity
   - 1.3. Availability
2. Is there a need for Information Security?
   - 2.1. Why do we need Information Security?
     - 2.1.1 Examples of InfoSec Breaches:
       - *i. British Airway's Customer Data Hack 2018*
       - *ii. The Bank Heist of 2013*
       - *iii. Cryptowall Ransomware Case*
3. What are the Information Security Laws in the United Arab Emirates?
   - 3.1. Information Security Standards and Legislations
     - 3.1.1 Principal Data Protection Laws in UAE
       - i. On-Shore Regulations
       - ii. Sector-Specific Regulations
         - *a. Cyber Crimes*
         - *b. Federal Credit Information Law*
       - iii. Free-zone Regulations
         - *a. Dubai International Financial Centre (DIFC) Regulations*
         - *b. Abu Dhabi Global Market (ADGM) Regulations*
         - *c. DHCC under the Health Data Protection Regulations No 7 of 2013*
     - 3.1.2 Government Data Protection Regulations
       - i. Data Security Regulation (The UAE Cabinet Resolution No 12 of 2013)
       - ii. The National Electronic Security Authority (NESA)
       - iii. In the Emirate of Dubai
         - *a. Dubai Data Law 2015*
         - *b.* In the Emirate of Abu Dhabi
     - 3.1.3 Corporate Security Standards
       - i. SO/IEC 27001
       - ii. Payment Card Industry Data Security Standard (PCI DSS)
4. What are the Information Security Legislations and Standards?
   - 4.1. Saudi Arabia
     - 4.1.1 Data Protection Law
     - 4.1.2 Information Security Regulations
       - *a.* Common information security policies
       - *b.* System Specific Policies
   - 4.2. Bahrain
     - 4.2.1 Data Protection Laws
     - 4.2.2 Information Security Regulations
       - *a. Information Security Clauses in Contracts*
5. What is the need for Information Security clauses for Contracts in UAE and other GCC Countries?
   - 5.1. Contractual Considerations for Information Security Contract/Clauses
     - 5.1.1 Responsibility
     - 5.1.2 Compliance
     - 5.1.3 Third Party Compliance
     - 5.1.4 Confidentiality
     - 5.1.5 Control of Use
     - 5.1.6 Permitted areas
     - 5.1.7 Data separation
     - 5.1.8 Adequate Risk Assessment
     - 5.1.9 Termination of Contract
     - 5.1.10 Subcontractor Relationships
     - 5.1.11 Warranty
     - 5.1.12 Damages
6. Conclusion

# A GUIDE TO INFORMATION SECURITY AND DATA PROTECTION LAWS IN GCC COUNTRIES

New challenges have arisen with the technological development along with the social and economic globalization. It can be said that our entire personal data is being stored in the gadgets we use. Internet today has brought millions of unsecured computer networks into continuous communications with other networks. With the advent of information being stored electronically, more and more people use online banking and shopping services, social media, location-based services, mobile services for their everyday activities. This results in the collection of an enormous amount of digital trail of personal data of these users which are left all over the internet. The security of each computer's information depends upon the level of security of other computers connected to it.

In the recent years, with the realization of the importance of Information Security to both national security and the corporate world, awareness of the necessity to improve Information Security has grown and is ever increasing.

In this guide, we will address the following questions regarding Information Security:

I. What is Information Security?

II. Is there a need for Information Security?

III. What is the relevant legislation for information security in the UAE and other GCC countries?

IV. What are information security agreements/ clauses and what needs to be added to these clauses/agreements?

## 1. What is Information Security?

In the earlier stages, Information Security was a simple process composed of predominantly physical security of documents and its classification. The primary threat faced by companies were theft of equipment, product espionage of the systems and sabotage. One of the earlier documented cases of security problems occurred in early 1960, where the systems administrator was working on the *'Message of the Day'* and another administrator was editing the password file, when a software glitch mixed the two files, causing the entire password file to be printed in every output file.

With the growing concern about State's engaged information warfare and the possibility that business and personal information systems being threatened if left unprotected has made Information Security (InfoSec) emerge as a method to ensure the confidentiality of the available data and also the availability of technology enabling the delivery and processing of that data. In simple terms, it can be explained as the protection of information and systems from unauthorized access, disclosure, alteration, destruction or disruption.

***It can be said that the main objectives of Information Security are:***

### 1.1 Confidentiality

It refers to the preventing unauthorized access or disclosure of information and providing its protection. Confidentiality means ensuring that the individuals authorized are able to access the information and those who are not authorized are prevented.

### 1.2 Integrity

It is the protection of information from unauthorized alteration or destruction, and ensuring that the information

*"If you exchange information internationally, you must strengthen data protection. Those are two sides of the same coin."*

***– Gijs de Vries***

and its systems are uncorrupted, accurate and complete.

### 1.3 Availability

It means to ensure that the information is available in a timely manner and there is reliable access to and use of the information and the information systems, at the same time, protect the information and information systems from unauthorized disruption.

## 2. Why do we need information security?

### 2.1. Why do we need Information Security?

A fundamental aspect for the success of our economy and society is data, and the protection of the same from cybercriminals has become the need of the hour in today's cyber world.

Advanced Persistent Threat (ADT) is a well-resourced systematic attack perpetrated by competing states and cyber criminals who aim at state secrets, corporate espionage, and theft of sensitive data. ADT has added to the breaches of millions of the individual personal, health and financial information, making it essential for institutions that collect and use personal data to develop and sustain a comprehensive security system in order to protect itself against such attacks.

For the security of individuals and the survival of enterprises, it is paramount to secure information resources and protect personal information from being exposed to groups or individuals with malicious intentions. While businesses struggle to survive amidst these critical issues surrounding information security and the increased risk of serious data breaches, governments are also changing their data protection laws so as to adapt and secure itself against these new risks that arise every day.

When companies entrust business partners and vendors with the company's confidential information, the company is also entrusting them with all control of the security measures for the company's data. Such a trust cannot be blind.

### 2.1.1 Examples of InfoSec Breaches:

*i. British Airway's Customer Data Hack, 2018*

The British Airways recently announced that over 380,000 payment card details and personal data of customers were compromised following a 15-day hack attack from 21st of August 2018 to 5th September 2018 and warning the customers to contact their banks immediately in order to secure the same.

*ii. The Bank Heist of 2013*

In 2013, the world witnessed one of the biggest bank heists of the century. A team of cybercriminals stole $45 Million (AED 165 Million) from RAKBANK and Bank of Muscat by accessing the computers of their credit card processors. Once they gained access, they increased the available balance and withdrawal limits on prepaid MasterCards issued by the banks. They then distributed these counterfeit cards to "cashers" around the world enabling them to siphon millions of dollars from ATMs. This included over 36,000 transactions which were committed in a matter of 10 hours.

*iii. Cryptowall Ransomeware Case*

Cryptowall is a file-encrypting ransomware program which was used by its creators to make over $1 million by infecting over 600,000 computer systems in 2014. Once gaining access into the computers, they encrypted the sensitive information files which were only decrypted when the owners paid the ransom. Even though Cryptowall had been spreading since 2013, it had been overshadowed by Cryptolocker, which is another ransomware program. When the threat of Cryptolocker was mitigated, the makers of Cryptowall stole the data by accessing computers through various tactics including spam emails with malicious links and attachments, drive-by-download attack for infected sites with exploit kits and through installation through other malware programs already installed and running on compromised computers.


*"You can't hold firewalls and intrusion detection systems accountable. You can only hold people accountable."*
*- Daryl White*

## 3. Q. What Are The Information Security Laws In The United Arab Emirates?

### 3.1. Information Security Standards and Legislations

The UAE has no consolidated information security law, but through various legislations, several standards have been placed to ensure that both private and public organizations maintain a certain standard of information security.

The information security in the UAE can be divided into three standards:

I. Personal Data Protection Regulations

II. Government Data Protection Regulations

III. Corporate Information Security Standards

#### 3.1.1. Personal Data Protection Laws in the UAE

Personal Data refers to the data of an individual who can be identified, directly or indirectly, particularly relating to an identification number or specific factors to their biological, mental, economic, cultural, biometric or social identity. The personal data of individuals are regulated across various legislations. Some of the key regulations are mentioned below:

*i. On-Shore Regulations*

The following laws affect the data protection law of the UAE:

*a.* Article 378 of the Penal Code (Law No 3 of 1987) – Punishment for violation of private or familial life by recording or transmitting private conversations or by capturing images of a person in a private place.

*b.* Article 379 of the Penal Code punishes the unauthorized disclosure or use of information or secrets accessible to a person, by virtue of his profession or position.

*c.* Article 31 of the UAE Constitution of 1971 protects the general *right to privacy* with regard to correspondence and other communication.

*ii. Sector-Specific Regulations*

Certain sector-specific regulations have been placed for the protection of data in the respective sector, such as:

*a. Cyber Crimes*

Federal Law no 5 of 2012, in relation to information security, prohibits the following:

1. Unauthorized access to an Information Technology (IT) system to obtain personal or government information;
2. Hindering access to an IT system or disabling an IT system by introduction of spam emails and virus programs; and
3. Hacking into IT systems.

*b. Federal Credit Information Law*

The Credit Information Law (Federal Law No 6 of 2010) and the following Cabinet Regulations No 16 of 2014 (the Regulations) provides for the following:

1. Prohibition on the collection and circulation of data or details relating to the private personal life, opinions, beliefs, or health;
2. Requires the consent of data subjects before issuing any credit information reports relating to such subject;
3. Restricts the use of information gathered only for the purpose for which it was provided for; and
4. Places obligation on the holder of credit information to ensure the confidentiality of such information.

*iii. Free-zone Regulations*

Certain free-zones have their own regulation for the protection of personal data, which applies only within the territorial limits of the respective free-zones. Below are the principal regulations in place by the DIFC, ADGM and the DHCC:

*a. Dubai International Financial Centre (DIFC) Regulations*

The regulations that regulate and protect individual data in the DIFC are:

*"If privacy is outlawed, only outlaws will have privacy."*
*– Philip Zimmermann*


1. DIFC Law no 1 of 2007 (amended by DIFC Law No 5 of 2012)
2. DIFC Data Protection Regulation (consolidated version No 2 of 2012)

*b. Abu Dhabi Global Market (ADGM) Regulations*

ADGM has enacted the following regulations in order to safeguard personal data and its dissemination:

1. Data Protection (Amendment) Regulations 2018
2. Data Protection Regulation of 2015- which is consistent with the organization for Economic Co-operation and Development's Guidelines and the European Union's Directives on protection of privacy and personal data.

*c. DHCC under the Health Data Protection Regulations No 7 of 2013,* provides for detailed provisions for the protection of patient data and patient health information including information about the patient's medical history, health, disabilities and donation of parts and bodily substances.

### 3.1.2. Government Data Protection Regulations

*i. Data Security Regulation (The UAE Cabinet Resolution No 12 of 2013)*

This outlines how data belonging to the UAE Federal Government, authorities, ministries and other official entities must be stored, treated and transmitted.

*ii. The National Electronic Security Authority (NESA)*

The information assurance standards by NESA UAE requires the implementation of information security controls for the protection of information assets and supporting systems across the UAE entities. It applies to information pertaining to the Government of the UAE and its Emirates.

Organizations complying with the NESA standards can ensure the protection of their information assets by mitigating information security risks that are identified and the implementation of effective controls along with the compliance with the UAE regulations.

*iii. In the Emirate of Dubai*

*a. Dubai Government Information Security Resolution (DGISR)*

DGISR is an Information Security Regulatory authority, developed to maintain information security to maintain information security standards in Dubai in line with the International Standards of Compliance. These standards from the Dubai Smart Government mandates the Dubai government entities to implement controls and requirements provided in the standard, ensuring the appropriate balance of confidentiality, integrity, and availability of information assets.

Government entities following these standards have several advantages including: conforming to the requirements of ISO 27001 and ISR; ensure that risk assessments are conducted on all information systems; develop information security policies; identify the accountability for maintenance of information security; respond to information security incident and establish appropriate to assess and determine the compliance and effectiveness of these standards.

*b. Dubai Data Law 2015*

Dubai Law, No 26 of 2015, regulates the Dissemination and Exchange of Data in the Emirate of Dubai. It provides for:

1. Applies to Data Providers- including Federal Government entities and Local Government entities possessing data relating to the Emirate of Dubai, as well as, individuals and entities (like sole proprietorships, companies and organizations) whether located in on-shore Dubai or in any of the Free-zones and who own, produce, exchange or publish data relating to the Emirate of Dubai;
2. Ensuring that the data gathered by the Dubai Government entities and the private sector are effectively shared amongst such entities so as to maximize


*"To competently perform rectifying security service, two critical incident response elements are necessary: information and organization."*

*- Robert E. Davis*

the benefits to Dubai's economy, resident and visitors; and

3. Includes managing data in conformity with the international practices and promoting transparency by establishing rules for data dissemination and exchange of data efficiently by the Federal Government entities and the local government entities.

*iv. In the Emirate of Abu Dhabi*

The Abu Dhabi Government Information Security Policy and the related Security Standards provide for comprehensive regulations regarding the Government Data in the Emirate of Abu Dhabi assuring the confidentiality, integrity, and availability of critical government information.

It defines the requirements for ensuring the security of all critical government information regardless o the medium of its existence.

All Government entities and other entities in Abu Dhabi, having access to or in possession of critical government information, are under this law required to:

***a.*** Categorize their information assets on the basis of importance and critical nature;

***b.*** Develop an information security program plan;

***c.*** Build required capabilities to monitor information systems and manage the security incidents that occur within the entity; and

***d.*** Regularly provide reports to the Abu Dhabi Systems and Information Center, who is responsible for assisting government entities in implementing their security programs.

### 3.1.2. Corporate Security Standards

Though there are no benchmark standards for the assessment of the information security regime of a company, it is the responsibility of the company to ensure reasonable and adequate information security standards and mitigate security risks to such information. In the event of any breach to the Information Security, the company shall be liable to compensate for any losses incurred by the breach, which is why companies generally use the various industry standards which have been developed and used as a basis to implement "reasonable" and "adequate" measures in the context of information security.

*i. ISO/IEC 27001*

ISO 27001 is a specification for information security management systems (ISMS), which is a framework of policies and procedures including all legal, physical and technical controls included in an organization's information security process.

ISO 27001 includes details for documentation, responsibility, management, internal audits, continuous improvement, and corrective and preventive measures. Though there are no mandatory specific controls for Information Security, ISO 27001 provides for a checklist of controls to be considered.

ISO/IEC 27002, is an accompanying code of practice to the 27001 standards, describing a comprehensive set of information security controls objectives and a set of security control practices that are acceptable. It contains 12 sections including risk assessment and management; a security policy; organization of information security, control of access, information systems acquisition, development, and maintenance compliance.

*ii. Payment Card Industry Data Security Standard (PCI DSS)*

PCI DSS is a security standard developed and administered collectively by major credit card companies such as Mastercard, Visa, and American Express. It includes standards that are globally acceptable and applicable to any person, business or organization (ranging from small to multinational organizations) handling credit card data. PCI DSS contains over 12


*"Information Security Officers must share more than hackers."*
*– Stephane Nappo*

overall requirements which are to be satisfied for compliance and are more detailed than the ISO 27001, such as requiring the maintenance of firewalls for the security of credit card data.

Though confined in scope to organizations handling credit card transactions, its detailed provisions provide a standard regime (especially technical) of good practical advice on several security issues for organizations that wish to set up information security regimes.

**4. Q. What are the information security legislation and standards in other GCC countries?**

In this section we examine the Information Security legislation and guidelines in three GCC countries, namely:

I. Saudi Arabia

II. Bahrain

### 4.1. Saudi Arabia

#### 4.1.1. Data Protection Law

Data protection law in Saudi Arabia largely depends upon the principles of Shari'a Law, but there are also certain sector-specific regulations protection personal data such as:

*i.* The Basic Law of Governance which provides that the telegraphic, postal, telephone and other means of communications shall be safeguarded and cannot be confiscated, delayed, breached or read.

*ii.* The Anti-Cyber Crime Law which prohibits the interception of information transmitted through information network, the intrusion of privacy by use of camera-equipment, illegal access to bank or credit data and unlawful access to computers amongst others.

*iii.* The Telecoms Act which protects the privacy and confidentiality of telephone calls and the information that is disseminated through public networks, by prohibiting the recording, disclosure or listening of the same.

#### 4.1.2. Information Security Regulations

The Information Security Policies and Procedures Guide was developed by the Computer Emergency Response Team – Saudi Arabia (CERT-SA) in the Communication and Information Technology Commission (CITC) and initiated under the Government Mandate No (81)- 191430/3/H as compulsory requirements to be followed by the Government Agencies of Saudi Arabia. The purpose of the guide is to assist the Government agencies in Saudi Arabia in developing their information security policies and procedures in a quick and effective manner, keeping in line with the relevant information security risks these agencies face.

Though it was primarily developed to be used by the Government agencies of Saudi Arabia for improving information security policies and procedures for their respective organizations, the standards provided in this guide can be used by other public and private sector organizations and entities in Saudi Arabia and abroad.

The guide states that it is the responsibility of each organization to develop and maintain their own security framework and ensure the compliance of relevant regulations. The framework also needs to protect people and information by:

*a.* Establishing the rules for the expected behavior of users, management and security personnel and system administrators;

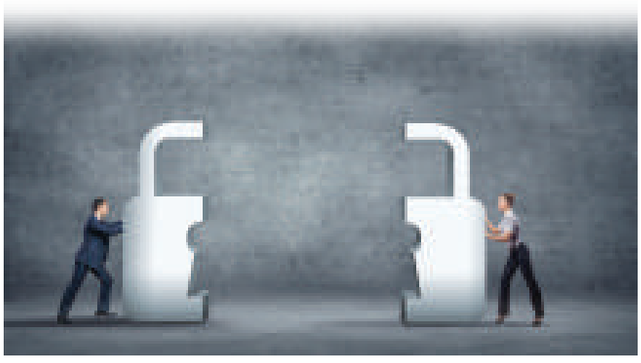
*b.* Authorization of security personnel to monitor, probe and investigate;

*c.* Defining and authorizing the consequences of violation as well as defining the organization's stance on security; and

*d.* Minimizing risk and track compliance with regulations.

On the basis of consideration of several factors such as the information security needs and the wide range of audience to be addressed in the organization, the guide classifies the information security policies into:

***"Security, is not about making IT perfect, but making customer lastingly satisfied and confident."***
***– Stephane Nappo***



*i. Common information security policies*

Which is categorized on the basis of the control group such as Access Control, Business Continuity, and Acceptable use policy. They pertain to the most common information security risks that apply to these organizations and identifies the specific group of audience targeted.

*ii. System Specific Policies*

They are categorized on the basis of specific types of systems identified in the guide such as Application, IT System, Networking and Physical Infrastructure, which assist in Government agencies to develop risk-based specific policies depending upon the information systems used and the confidentiality, integrity, and availability needs. Where applicable, these policies support three levels of information security requirements.

### 4.2. Bahrain

#### 4.2.1. Data Protection Laws

In Bahrain, there are several sector-specific data protection laws such as:

***a.*** Electronic Transactions Law (Legislative Decree No 28 of 2002) which protects the confidentiality of electronic records;

***b.*** Telecommunications Law (Legislative Decree No 48 of 2002) prohibits divulging of any confidential information;

***c.*** Decree No 64 of 2006 relating to the Central Bank of Bahrain and the Financial Institutions Law contains provisions regarding confidential information and the disclosure of such information.

However, on 19th of July 2018, a new law on Protection of Personal Data was published, which will come into effect on 1st of August 2019, and requires a variety of changes in how the businesses in Bahrain process information in Bahrain or about the residents of Bahrain. It applies to both natural and legal persons including corporates. The new law also criminalizes several acts, which are mostly subject to administrative penalties in other countries. The sanctions include imprisonment of up to 1 year and/or fines ranging from BHD 1000 to BHD 20,000 or a fine in case of corporate entities.

#### 4.2.2. Information Security Regulations

In the absence of detailed regulations in this regard, Information Security standards of companies in Bahrain are primarily based on ISO-27001 recommendations for the formulation of their Information Security Risk Management System (ISRM).

*i. Information Security Clauses in Contracts*

Organizations should perform several checks to ensure the adequacy of information security and privacy practices within business partners, vendors and other outsourced companies including the addition of Information Security clauses in contracts that specifies the information security policies to be mandatorily followed by the party.

## 5. What are the Information Security agreements/-clauses and what needs to be added to these clauses/agreements?

### 5.1. Q. What is the need for Information Security clauses for contracts in the UAE and other GCC countries?

Though there are no legal requirements to enter or include Information Security clauses or contracts, when data breaches or information security breaches occur, or the transparency violations are revealed, the organizations are likely to be held responsible for the same. In order contractually bind the other party to maintain the *confidentiality, integrity,* and *availability* of the company's information; to mitigate the risk of information security breaches; and to ensure the protection of the company in such a breach, Information Security Clauses/Contracts are a necessity. These contracts ensure that the other party, having access to your confidential information, will take all the steps necessary to prevent breaches and mitigate risks; abide by the organization's standards on Information Security measures and policies; and compensate the organization in case of any breach or loss.

*"True cyber security is preparing for what's next, not what was last."*

*-Neil Rerup*

When organizations share information, it is necessary to maintain the balance between disclosing the appropriate information. When information security breaches occur, there can be minor to catastrophic losses and damages, to be suffered by one or the other party.

### 5.2. Contractual Considerations for Information Security Contract/Clauses

When including information security and privacy requirements in contracts with other parties, ensure that enough details are provided to cover all issues but not so specific as to allow the party from avoiding a security activity merely because you did not specifically state it within the contract. It is recommended to include citations of specific regulations and laws that the organization must comply with in order to clarify to the other party of their requirement to comply with the same.

In order to ensure the utmost protection of the organization and its information, it is recommended to ensure that the following points are covered in the Information Security Agreements or Clauses in other Contracts:

#### 5.2.1. Responsibility

In all critical privacy and information security areas (including administration, technical support, privacy, awareness, and training), define which person or position shall be held contractually responsible for the information security and privacy issues and as the primary contact for all related communications.

#### 5.2.2. Compliance

A compliance clause, requiring the party to comply with all the relevant laws and regulations, applicable in international, national and state levels. It is recommended to spell out the particular obligations that require mandatory compliance. This ensures that the party contractually agrees and is bound to follow the regulatory requirements. The organization can also require the party to maintain information security and privacy policies in documentation. require the party to maintain information security and privacy policies in documentation.

#### 5.2.3. Third Party Compliance

It is also necessary, in the case of third-party contracts to ensure that the party agrees to comply with all the appropriate components of the organization's privacy and information security policies including physical security of premises, clearance of personnel, data security storage, handling of media.

#### 5.2.4. Confidentiality

This includes a non-disclosure agreement or clause with the parties including partners, other staffs and subcontractors.

#### 5.2.5. Control of Use

Contractually hold the other party bound to acquire the permission of the organization to use, access, replace or amend any purchased data list or production data for testing.

#### 5.2.6. Permitted areas

Limiting the access to data and assets by specifying:

*i.* Who can see;

*ii.* What kind of data is accessible; and

*iii.* The amount of such data that can be accessed.

#### 5.2.7. Data separation

Require physical and logical separation of data from other organizations' data, depending upon the amount and kinds of risk involved.

#### 5.2.8. Adequate Risk Assessment

It is necessary for companies to do Security Risk Assessments as part of the design and implementation of new resources for information and its changes. The organization can contractually require the party to provide a copy of at least an executive summary of the most recent risk assessments conducted by the other party, where the other party is a company.


*"Privacy and security are really important. We think about it in terms of both: You can't have privacy without security."*

*- Larry Page*

#### 5.2.9. Termination of Contract

Immediately upon the termination of the contractual relationship, require the other party to return and/or irreversibly destroy all of the company's data, as appropriate. It is also necessary to ensure that the party shall not continue to have access to the company's systems and data, so as to avoid the risk of such information being mishandled by such party.

#### 5.2.10. Subcontractor Relationships

Prohibit subcontractor relationships where the party has to provide any forms of access to the organization's data or system, without acquiring prior permission from the organization.

#### 5.2.11. Warranty

Ensure that the warranty clause is clearly worded in the standard contractual language as recommended by the organization's legal counsel including the addition of applicable regulatory measures.

#### 5.2.12. Damages

Apart from the recommendations from the acquisition department of the organization, ensure the addition of contractual liability of the party to reimburse the organization for any damages resulting from information security or privacy incidents involving the organization's data, that occur within the party's organization. For example, if an employee of the party, loses a laptop or hard drive with the organization's data.

Ensure that the value of loss includes the value of data and service time and not just of the hardware involved.

## 6. Conclusion

Entrusting your organization's data to another company, or outsourcing the data handling, processing and management is a risky business for your organization, and the cardinal principle is that it is the organization's responsibility to ensure that strong security follows such data. In the end, the ultimate responsibility for the security of the information lies upon the organization to whom it belongs. It is always safe to follow a strong security regime, rather than make headlines by the loss of information due to weak Information Security.

*"The payment for sins can be delayed. But they can't be avoided."*

*-Shawn Ryan*

## STA Law Firm's offices across GCC


**Abu Dhabi Office**

Advocates and Legal Consultants
23 A, Level 23 Tamouh Towers
Marina Square, Reem Island
Abu Dhabi, United Arab Emirates

Tel: +971 2 644 4330
Fax +971 2 644 4919

**ADGM Office**

3517, Al Maqam Tower
Abu Dhabi Global Markets Square
Abu Dhabi
United Arab Emirates

Tel: +971 2 644 4330
Fax +971 2 644 4919

**Dubai Office**

Advocates and Legal Consultants
Office 1904, Level 19, Boulevard Plaza,
Opposite Burj Khalifa
Dubai, United Arab Emirates

Tel: +971 4 368 9727
Fax +971 4 368 5194

**Sharjah Office**

48-1F, Next to Abu Dhabi Islamic Bank
Near Hamriyah Free Zone Headquarters,
Hamriyah
Sharjah, United Arab Emirates

Tel: +971 6 513 4270
Fax: +971 6 526 4027

**Bahrain**

Advocates and Legal Consultants
Level 22, West Tower
Bahrain Financial Harbour
King Faisal Highway
Manama
Kingdom of Bahrain

Tel: +973 1750 3045

**Qatar**

Level 22, Tornado Tower
West Bay, Doha
Qatar
PO Box – 27774

Tel: +974 44294827

**RAK Office**

Office 501-A, Level 5, Building 4
Ras Al Khaimah Free Trade Zone
Ras Al Khaimah,
United Arab Emirates

Tel: +971 7 204 2180

Fax: +971 7 204 2181

**Fujairah Office**

Creative Tower
Creative City - Media free zone
Fujairah,
United Arab Emirates

Tel: +971 7 204 2180

Fax: +971 7 204 2181


*For a free subscription request, you can e-mail us at:*
corporate@stalawfirm.com
*with your name and address.*
www.stalawfirm.com


ISBN 978 - 9948 - 22 - 445 - 7




Office 1904, Level 19,
Boulevard Plaza, Tower 1,
Opp. Burj Khalifa, Dubai
United Arab Emirates

Tel: +971 4 368 9727

corporate@stalawfirm.com
www.stalawfirm.com