وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT
AND COMMUNICATIONS

e-Commerce Guidelines
Technology

motc.gov.qa

E-Commerce Guidelines

Technology

Prepared by:

Ministry of Transport and Communications
(MOTC)
State of Qatar

2018/2019

About the Document

This document contains recommended guidelines for managing technology for e-commerce ecosystem in Qatar. The primary objective is to ensure that e-commerce businesses, financial institutions, IT service providers and logistics partners design and implement best technology practices. These guidelines should be used as a framework and adhered to when defining technology controls for the business.

Table of Contents

1. Introduction

1.1. Background

E-commerce (Electronic Commerce) is becoming more of a business imperative than ever before as consumer awareness and expectations evolve. The proliferation of high-speed broadband and the availability of a sophisticated Internet infrastructure and Web-enabled mobile devices present increased economic opportunities for government, businesses, and individuals that could have profound impact on how future business-to-business (B2B) and business-to-consumer (B2C) commerce is conducted.

When it comes to good e-Commerce practices, technology is the key. It plays a vital role in all aspects of implementing an efficient e-Commerce system and value chain. By keeping up to date with the latest technology-related best practices for your business, you can enhance security, and drive efficiency and sales, ensuring an improved customer experience.

1.2. E-Commerce

e-commerce is the direction of business activity when the process of providing customers with goods or services is done by means of electronic devices and the Internet. This sort of communication and finalization of sales adds some new aspects to data management, sales channels, advertising, presenting goods and services and moreover—enabling full cycle of commerce operations, including payments, delivery and refunds.

1.3 Key Stakeholders

With growing use of technology and information, Organizations should envisage the need for technology and safeguarding the interests of following key -stakeholders:

- Customers/subscribers who need confidence in the organization's network and the services offered, that includes availability of services, and protection of their personally identifiable information;
- Regulatory authorities who demand security by legislation and/or directives, in order to ensure availability of e-commerce services and privacy protection;
- Vendors (such as IT Service providers, logistics partners, payment service providers) who need information security to safeguard the day to day operations related to the job functions and to meet their obligations to the customers; and
- E-commerce merchants, retailers and financial institutions who need to ensure that the business objectives are fulfilled, the overall posture of the organisation highlights information security as a culture, the overall investors' confidence is bolstered, the vendors and customers feel a goodwill and comfort with the services.

2. Technology Guidelines

2.1 Information Security

This guideline is applicable to all the information and information systems, throughout their lifecycle across ecommerce merchants, IT service providers, logistics partners, and financial institutions (hereafter referred to as Organizations) wherever the information and information systems reside.

The objective of this guideline is for implementation of information security controls organization wide. Organizations shall be committed to provide comprehensive protection to its information assets against the consequences of breaches of confidentiality, failures of integrity and/ or interruptions to their availability. The Organizations shall define appropriate security frameworks and security organization structure, define responsibilities, and identify resources to manage information security throughout the organization.

The management shall demonstrate leadership and commitment with respect to the information security by:

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- Ensuring the integration of the information security requirements into the organization's processes;
- Ensuring that the resources needed for meeting information security objectives and requirements are competent and made available;
- Communicating the importance of effective information security and of conforming to the information security management system requirements to users as well as vendors;
- Ensuring that the information security achieves its intended outcome(s);
- Define and implement measures to monitor effectiveness of the information security objectives within the organization;
- Promoting continual improvement;
- Management shall consider implementing or aligning the information security requirements within their Organization based on the criticality of the activities performed to Government mandates, policies, guidelines and various international standards such as ISO 27001, PCI DSS etc.; and
- Supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Top management shall establish an information security policy that:

- Is appropriate to the purpose of the organization;
- Includes information security objectives or provides the framework for setting information security objectives;
- Includes a commitment to satisfy applicable requirements related to information security; and
- Includes a commitment to continual improvement of the information security management system.

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated. Top management shall assign the responsibility and authority for:

- Ensuring that the information security conforms to the requirements of this International Standard; and
- Reporting on the performance to top management.

2.2 Identity Management – Sign In

This guideline is applicable to all the applications, information and information systems of e-commerce Organizations.

Identity management addresses proper use of credentials for the unique identification and authentication of users. As organizations grow and add services, and integrate new business functions such as joint ventures and multiple span projects, controlling who is accessing company information resources is becoming an even more difficult task. As the scope of access control continues to grow and span across multiple systems and multiple applications, each system could be using a different method of access control and user authentication. Access to information assets shall be controlled based on business and security requirements, and commensurate with the organizational policies. Access controls shall be applied on the principle of – 'deny all unless explicitly permitted' to protect the information assets from unauthorized access. The objectives of the Identity Management are to:

- Restrict access to information assets as per the business requirement;
- Prevent unauthorized access to information systems, network services, operating systems and information held in database and application systems;
- Ensure that the mobile computing and teleworking facilities are protected with appropriate security controls.
- Ensure that information access controls are implemented to meet any relevant contractual requirements, as applicable.

2.3. Payment Confirmation

Ecommerce payments, being one of the most rapidly changing ecosystems in the world, is constantly in a state of flux. With the continuous evolution and increasing adoption of digitized living (i.e. a lifestyle in which internet-connected devices allow people to work, shop, play, create, share, inform, communicate, and transact in an integrated manner, on their own terms, 24/7, across the globe), consumers expect greater speed and convenience. And not only in the payments experience, but also in the way of interaction and consuming other financial services.

This guideline highlights guidelines for managing payment security by ecommerce merchants and financial institutions; and highlighting security practices for customers. This guideline is applicable to all e-commerce Organizations regulated by Ministry of Transport and Communications (MoTC). This guideline aims to take into account all the payment modes that are adopted across Organizations.

Various payment instruments that ecommerce merchants provide in order to serve the customers seamlessly:

- Credit Cards: Credit cards are widely used internationally, and enjoy a status of being widely accepted as common payment method. However, there has been a gradual decline in credit card usage internationally, as e-wallets and other alternatives gain more ground. In wake of this, loyalty cards have taken large strides towards growth.
- Debit Card: On top of the card being useful for offline payments, debit cards are increasingly used online as well. Functioning in much the same way as a credit card, but without several risks of debt, the debit card has become popular.
- E-wallet: An e-wallet is a digital tool for consumers to store their money. It can be seen as the digital equivalent of our physical wallet. E-wallets can contain (pre-registered) credit cards, debit cards, gift and loyalty cards and provide access to alternative payment

methods like online bank transfers. Some e-wallets allow the consumer to preload money into their wallets. E-wallets provide improved payment experience and simplify online and mobile checkout.

- Online Banking e-Payments (OBeP): The Online Banking e-Payments (OBeP) scheme is a type of payments network designed to facilitate online bank transfers. In an OBeP scheme, the consumer is authenticated in real-time by the consumer’s financial institution. The availability of funds is validated in real-time and the consumer’s financial institution provides guarantee of the payment to the merchant in case the payment is made as a credit transfer (push payment): the consumer/buyer initiates the payment. The merchant receives a real-time guarantee so he can continue with the fulfilment process.
- Prepaid payment instruments: Pre-paid payment instruments are payment instruments that facilitate purchase of goods and services, including funds transfer, against the value stored on such instruments. The value stored on such instruments represents the value paid for by the holders by cash, by debit to a bank account, or by credit card.
- Cash payments / Cash on delivery: Cash on delivery (COD) is a payment method in which ordered goods are carried to the buyer’s place but are handed over only upon full payment. In Qatar, most payments are made on a cash-on-delivery basis, and there are limited e-payment methods (debit cards, prepaid cards, digital wallets, etc.).

2.4. Design Best Practices

Design best practices and secure development ensure that the code and processes that go into developing applications are secure. Secure development entails the utilization of several processes, including the implementation of a Security Development Lifecycle (SDLC) and secure coding itself.

The objective of this document is to specify the controls that need to be incorporated and validated in various applications to control access and protect the confidentiality, integrity and availability of the information processed by or stored in these applications.

These guidelines takes into account information security related requirements should be included in the requirements for new information systems or enhancements to existing information systems across ecommerce merchants and financial institutions (hereafter referred to as Organizations) to ensure that information security is designed and implemented within the development lifecycle of information systems.

2.5 Accessibility

This guideline helps in managing, and delivering accessible applications for organizations. The W3C Web Accessibility Initiative (WAI) provides a set of accessibility standards that are commonly recognized by governments and organizations from around the world. These include:

- Web Content Accessibility Guidelines (WCAG) 2.0 is applicable to all web content and applications, including on mobile, television, and other delivery channels.
- Authoring Tool Accessibility Guidelines (ATAG) 2.0 is applicable for websites that provide users the opportunity to generate content, such as adding comments, posting to forums, or uploading images or videos. ATAG is also relevant if your organization provides tools, such as CMS’s, for staff or customers to manage websites and content.
- User Agent Accessibility Guidelines (UAAG) 2.0 is applicable when additional plug-ins, such as media players, are provided to deliver content or when custom controls are developed to provide non-standard functionality.

3. Detailed Guidelines

3.1 Information Security

➢ Information Asset Management and Information Classification

- **Information Asset Management**

  This section provides the guidelines for achieving and maintaining appropriate protection for organizational assets. It also specifies the guidelines for identifying critical details of an asset, and understanding the importance of asset to provide an adequate level of protection for safeguarding.

  A designated owner should be selected, by the heads of all function/department/group (or their designated representative) for each asset. The information assets should be tracked across its lifecycle and rules concerning the acceptable use of information assets shall be identified, documented and implemented. These information assets shall be returned upon termination of the employment, contract or agreement. Organization shall take appropriate measures to prevent misuse of its assets and ensure their protection.

- **Information classification**

  Information assets of any organization are of utmost importance, and confidentiality, integrity and availability of these shall be maintained appropriately. Organizations should ensure that:

  - Information assets should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification;
  - Owners of information assets should be accountable for their classification. The classification scheme should include conventions for classification and criteria for review of the classification over time. The level of protection in the scheme should be assessed by analysing confidentiality, integrity and availability and any other requirements for the information considered; and
  - Classification should be included in the organization's processes, and be consistent and coherent across the organization.

➢ Access Control

- An access control policy should be established, documented and reviewed based on business and information security requirements.
- Access to information assets shall be controlled based on business and security requirements, and commensurate with the information asset classification. Access controls shall be applied on the security principle of 'deny all unless explicitly permitted' to protect the information assets from unauthorized access. The Organizations may refer the following for detailed guidance:
  - Organizations shall implement a formal registration and revocation procedure for granting and revoking access to all information systems and services;
  - Both logical and physical access controls should be considered together;
  - Organization shall control the allocation of passwords through a formalized management process;
  - Organization shall periodically review user access rights through a formalized process;
  - Organizations shall define and implement measures in place to safeguard end user access and passwords;
  - Organization shall limit access to third party vendors to critical systems and if required shall be provided after appropriate validations have been performed;

  - Organization shall implement “Role Based Access Control” and the same shall be applicable for all systems and users including customers / end users / privilege users; and
  - For critical e-commerce transactions Organizations shall implement multi-factor authentication prior to granting access to Organization systems.

- **User responsibilities**
  - Organization shall ensure that the users follow good security practices in the selection and use of complex passwords;
  - Organization shall implement and adopt a clear desk policy for papers, removable storage media; and
  - Organization shall have a clear screen policy for information processing units. Computers and terminals should be left logged off or protected with a screensaver when unattended and should be protected by key locks, passwords or similar controls when not in use.

- **Network access control**
  - Users shall only be provided with access to the network services that they have been specifically authorized to use. It shall be ensured that appropriate authentication methods are used by remote users in order to gain the access; and
  - Organization shall apply segregation in networks where it concerns groups of information services, users and information systems.

- **System and application access control**
  - Organization shall control the access to systems and applications in accordance with access control policy and through a secure logon procedure;
  - Use of privileged access and reviews shall be through a formalized process;
  - Strong and complex passwords shall be used to gain the access;
  - Organization shall implement further stringent controls for users with privilege access;
  - Activities of all privilege access users shall be recorded and monitored on a periodic basis;
  - Utility programs that might be capable of overriding the system and application controls shall be restricted and controlled; and
  - Organization shall control & restrict the access of program source code.

➢ **Human Resources Security**

- This guideline aims to ensure that the employment shall be in accordance with relevant laws, regulations such as National Information Assurance Policy, National ICS Security Standard and as per the business requirements. It outlines that the users are suitable for the roles they are hired for and they are made aware of their responsibilities for protecting confidentiality and integrity of information assets. It specifies the information security requirements that should be integrated in the HR processes during recruitment, employment and separation. This guideline is to address the risks of human error, theft, fraud, or misuse of facilities and assist all personnel in creating a secure computing environment.

- It shall be ensured that:
  - o Users understand their responsibilities related to Information security;
  - o Background verification shall be in-place as per the approved process;
  - o A confidentiality / non-disclosure agreement is signed by users at the time of joining;
  - o Users are trained to use information systems securely; and
  - o Ensure that users exit as per the approved process.
- Organizations shall initiate a disciplinary process for users who are found to be indulged in the security violation & breaches.

➢ **Physical and Environmental Security**

- This guideline provides direction for the development and implementation of appropriate security controls required for the protection of information assets and processing facilities of an Organization from physical and environmental threats. Information processing facilities, data centres, operations centres, disaster recovery site, and other sites as determined by management, shall be suitably protected.

- **Secure areas**
  - o Security perimeters shall be defined and used to protect areas that contain sensitive or critical information and information processing facilities; and
  - o Organizations shall design and apply physical protection against external and environmental threats, such as, unauthorised access, damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disasters.

- **Equipment security**
  - o Equipment security controls shall be implemented to prevent loss, damage, theft, or compromise of information systems and interruption to Organization's activities;
  - o All equipment shall be protected against environmental threat, unauthorised access, power failures and other similar disruptions caused by failures in supporting utilities;
  - o Unattended equipment such as servers, network, wireless and telecom devices shall be stacked in secure enclosures;
  - o In cases where the equipment's are hosted on cloud or a third party premise, the Organization shall ensure that the Cloud service provider or the third party ensures implementation of controls in line with Organization Information Security Policy;
  - o All equipment while in transit such as backup tapes etc. shall be appropriately protected including physical and environmental security aspects;
  - o All cables, including power and network cables, shall be protected from damage or unauthorised interception;
  - o Organizations shall apply security to off-site equipment to limit the risk of working outside the organizational confines;
  - o Organization shall implement a secure disposal process and any re-use of equipment shall have valid check points to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal; and
  - o Any removal of information assets off the Organization's premises should require prior authorization.

- **Operations Security**
  - This guideline provides the directions to ensure appropriate and secure operations of information processing facilities. This should reduce opportunities for unauthorized or unintentional modification or misuse of Organizations information assets.
  - **Documented Operating Procedures**
    - Organization shall document procedures of operational activities associated with information processing and communication facilities;
    - These documents should be made available to the users for their use on need basis; and
    - Operating procedures and the documented procedures for system activities should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.
  - **Change Management**
    - Organization shall control the implementation of changes to information processing facilities and systems;
    - Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes;
    - All authorized changes to any information processing system must go through the change management process;
    - All logs of changes must be maintained and reviewed on a periodic basis; and
    - The change records shall be maintained as in accordance with relevant laws, regulations such as "The National Information Assurance Policy and the National ICS Security Standard" and as per the business requirements.
  - **Capacity Management**
    - Organization shall identify capacity requirements, taking into account the business criticality of the concerned system;
    - System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems;
    - To ensure the required system performance, Organization shall monitor and tune the use of system resources; and
    - Projections related to future capacity requirements shall be considered to optimise the system resources.
  - **Segregation of Duties**
    - Organizations shall segregate conflicting duties and areas of responsibility to reduce opportunities for unauthorized or unintentional modification or misuse of the Organization's information assets; and
    - Care should be taken that no single person can access, modify or use information assets without authorization or detection. The initiation of an event should be separated from its authorization.
  - **Separation of Development, Testing and Operational Environments**
    - Organization shall have separate development, test and operational zones to reduce the risks of unauthorized access or changes to the operational system; and

  - The level of separation between operational, testing, and development environments that is necessary to prevent operational problems should be identified and implemented.

- **Malicious Code and Malware Protection**

  Organizations shall to:

  - Implement adequate controls to detect, prevent and recover against malicious codes and malware;
  - Implement controls against the use of mobile code;
  - Ensure appropriate safeguards be implemented in the information systems to prevent the execution of unauthorised mobile code;
  - Prevent or detect the use of unauthorized software (e.g. application whitelisting); and
  - Define procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks.

- **Backup**

  - A backup policy should be established to define the Organization's requirements for backup of information, software and systems;
  - Organization shall backup copies of information, software and system images and test the same regularly in accordance with an agreed backup policy; and
  - Adequate backup facilities should be provided to ensure that all essential / critical information and software can be recovered following a disaster or media failure.

- **Logging and Monitoring**

  - Organization shall enable the event logging as per the system configurations requirements and manufacturer's specifications;
  - The logging should record faults, exceptions, system events, security events etc. Controls shall be implemented to protect the logs against tampering and unauthorized access;
  - Activities of system administrator and operator shall be monitored in accordance with relevant laws such as The National Information Assurance Policy and the National ICS Security Standard, National Cyber Security Strategy, QCB guidelines on Banking supervision rules and as per the security requirements;
  - All clocks with relevant information processing systems or security domain shall be synchronized to a single reference time source; and
  - Organization shall keep a record of all the operation and maintenance command logs as per the license condition.

- **Vulnerability and Software Management**

  - Organization shall develop and maintain the control to obtain information about technical vulnerabilities using vulnerability scan and network penetration test of information systems being used and its exposure;
  - Organization shall ensure that periodic review of configuration of infrastructure including network devices and applications is undertaken to identify any vulnerabilities;

  - o Action to minimise the exposure and associated risk shall be taken appropriately in timely manner; and
  - o Periodic actions to fix problems and to prevent such problems from reoccurring shall be taken.

- **Network Security Management**
  - o Organization shall manage and control the network to protect information in systems and applications;
  - o Segregation in networks shall be implemented by grouping the information services, users and information systems;
  - o Organization shall implement security controls on the network to ensure that information through the critical network systems is encrypted;
  - o Organization shall ensure that event logs for network devices monitored and appropriate measures are implemented to identify any security incidents that may / have occurred;
  - o Organization shall ensure that the security of network services is defined and included in any network services agreements, either in-house or outsourced. This includes security features, service levels and management requirements of all network services; and
  - o Network hardening shall be performed as a continuous improvement to secure the configurations.

- **Mobile Devices and Teleworking**
  - o Organization shall implement appropriate security measures against the risks of using mobile devices;
  - o Organization shall have the security measures to protect information for teleworking activities; and
  - o Remote access from foreign location shall be only on need basis.

- **Information Collection and Transfer**
  - o Organization shall obtain the consent of an individual (end user) before collecting his identity information for the purposes of authentication and should ensure that the collected information is used solely for the purpose of user authentication;
  - o Organization shall protect the transfer of information through the use of all types of communication facilities, to include electronic messaging, internet usage and physical media in transit; and
  - o Organization shall have a control for the secure transfer of the business information with external parties. Confidentiality or non-disclosure agreements shall be in place for the protection of the information transfer.

- **Cryptography**
  - o Organization shall use cryptographic controls in accordance with relevant laws and regulations such as the National Information Assurance Policy, and as per the security requirements. Key management control involving digital certificates and cryptography keys shall be developed and implemented to protect the keys in the lifecycle.

- **System Acquisition, Development and Maintenance**
  - **Security Requirements of Information Systems**
    - Adequate security related requirements shall be identified and included while developing new information systems or enhancements of the existing information systems;
    - Organization shall ensure the secure development of software and systems by applying the security controls to the development processes and by building the secure development environment. Change management process shall be used to control the changes in the development lifecycle;
    - Organization shall ensure a continuous improvement to secure the application services and transactions on public networks such as Internet;
    - For the induction of network elements in network, the network elements shall be tested as per relevant International Security Standards, as appropriate. e.g. standards, for Information Security Management System against ISO 27000 series standards;
    - The copies of test results and test certificates / reports shall be stored for a defined period from the date of procurement of equipment;
    - Contemporary security related features and features related to communication security shall be defined and implemented into the network. A list of security features, equipment, software etc. shall be maintained till they are in use;
    - Organization shall perform a technical review and test of applications following an operating system change or upgrade to ensure there is no adverse impact on organizational operations or security. Organization shall impose restrictions on changes to software packages in order to limit changes, discourage modifications to software packages and impose strict control on modifications;
    - Organization shall establish the secure system engineering principles like hardening, testing etc. and shall be applied to information systems. Organization shall monitor and supervise outsourced software development, if application is developed by the outsourced vendor;
    - Appropriate system security testing and system acceptance testing (user acceptance test) shall be performed to test the information systems before release to production environment; and
    - The test data used for testing shall be suitably protected and controlled.

- **Vendor Security**
  - Vendors are those who are contracted to supply hardware, software, managed services to manage the technical operations (like network, IT etc.), managed services to manage the business processes & operations (like call center, bill printing, invoice processing, logistics etc.) and/or in combination of any of those as specified above. Organizations shall follow the below guidelines to ensure safe and secure vendor relations
    - Organizations shall agree and document information security requirements for mitigating the risks associated with vendor’s access to the organization’s information assets;
    - Agreements with vendors to include requirements to address the information security risks associated with information and communications technology services and product supply chain;
    - Organizations should regularly monitor, review and audit vendor service delivery; and

- o Changes to the provision of services by vendors, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

➢ **Information Security Incident Management**

- **Management of Security Incidents and Improvements**
  - o Organizations shall have a documented process to ensure a quick, effective and orderly response to information security incidents. Information security events based on the qualification shall be reported to management on a timely basis;
  - o Organizations shall provide a mechanism to users to report any observed or suspected security weaknesses in systems or services;
  - o Organizations shall report information security incidents, frauds to the QCERT within 72 hours without undue delay;
  - o In case of delays, the Organization shall provide appropriate justification; and
  - o A knowledge base shall be created based on the learning from information security incidents.
  - o Appropriate controls shall be applied to identify, collect, acquire and preserve the information, which can server as evidence. Network forensics shall be performed on the qualified security incidents to identify the exposure and root cause.

➢ **Information Security Continuity Management**

- o Organization shall plan and implement information security continuity that addresses the information security requirements needed at the time of adverse situations;
- o Organization shall develop and maintain business continuity plans to ensure the continuity of the operations in adverse situations;
- o Appropriate redundancies shall be built to meet availability requirements as per the business requirements; and
- o Continuity plans shall be tested and improved (if needed) on a regular basis to ensure that they are effective and up to date.

➢ **Information Security Compliance Management**

- o All relevant legislative statutory, regulatory, contractual requirements and the Organization’s approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the Organization;
- o Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products;
- o The organization’s shall independently review its approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) at planned intervals or when significant changes occur; and
- o Information systems shall be regularly reviewed for compliance with the organization’s information security policies and standards.

- **Internal Audit**
  - The organization shall conduct internal audits at planned intervals to provide information on whether the information security framework conforms to:
    - Self-defined requirements for information security management; and
    - The requirements of any relevant Standards such as ISO 27001:2013, PCI DSS, QCB Framework etc.
    - Organization shall ensure that internal audit plan is effectively implemented and maintained; and
    - Organizations should ensure that the results of the audits are reported to relevant management.

- **Best Practices for Securing e-Commerce**
    - Use TLS 1.1 or higher when transmitting cardholder data internally (for example, at cardholder data ingress and egress points) throughout the network;
    - Due to the dynamic nature of e-commerce environments and frequent changes to websites and web applications, consider implementing a web application firewall (WAF);
    - It is also recommended that firewall rules be configured to ensure unwanted traffic does not access (both ingress and egress) the network. It is important to understand the type and nature of any firewalls installed in a service provider environment that controls access to services or environments provided to the merchant;
    - Regularly review any links (such as URLs, iFrames, APIs etc.), from the merchant's website to the payment gateway to confirm the links have not been altered to redirect to unauthorized locations;
    - It is recommended the merchant check with its service provider to ensure anti-virus/anti-malware software is running on the systems provided to the merchant. If the service provider is not running antivirus software on the merchant's behalf, it is recommended the merchant understand why and implement a solution of its own for those systems. It is also recommended a merchant have AV software running on the systems it manages; and
    - Merchants are advised to ask their service providers about the intrusion-detection/prevention systems and file-integrity monitoring in place. They are also advised to ensure their own systems are being monitored for intrusions.

- **Best Practices for End User Security**
    - End users shall update their passwords regularly and keep a password that is complex (combination of special characters, alphabets and numbers), to guess;
    - Users shall never disclose their information (such as Account Number, PIN number, credit card details etc.) over telephonic calls as this can be a social engineering attack;
    - Users shall practice caution while accessing emails from unknown sender and always verify the source before clicking on any links that might be embedded in the mail;
    - Users shall always use antivirus software on personal devices;
    - Users shall keep the operating systems and software on their devices up to date;
    - Regularly review online accounts and credit report;

  - While linking social media accounts, users should thoroughly read and understand the privacy policy of the e-commerce merchant, and be aware of how your information can be used;
  - The highest available level of privacy and security settings should be selected and activated on any social media site;
  - Avoid the use of public Wi-Fi networks, which are target-rich for cyber thieves;
  - Users shall regularly back up files onto external drive (to safely restore, in case of an incident);
  - Engage with verified social media pages and use official mobile apps linked from an official web site;
  - Inform the bank of changes in the mobile number to ensure that SMS notifications are not sent to someone else; and
  - As a best practice options to "Remember my card number" on websites where transactions are conducted should not be used.

3.2 Identity Management – Sign In

- **Identity Management for Organizations**
  - A formal identity management framework or policy that is approved by the Top Management shall be in defined and implemented;
  - A formal user registration and de-registration process shall be implemented to enable assignment of access rights;
  - Unique user identity shall be assigned to enable users to be linked to and held responsible for their transactions;
  - The use of shared identities should only be permitted where they are necessary for business or operational reasons and shall be approved and documented;
  - User IDs of users who have left the organization shall be immediately disabled or removed;
  - User IDs that are no longer required shall be periodically identified and removed/ disabled. Organizations should ensure that such user IDs are not issued to any other users;
  - A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services;
  - The process for assigning or revoking access rights granted to user IDs should include:
    - Obtaining authorization from the management/owner of the information system or service for the use of the information system or service;
    - Verifying that the level of access granted is appropriate to the Organization's access policies;
    - Ensuring that access rights are not activated before authorization procedures are completed;
    - Maintaining a central record of access rights granted to a user ID to access information systems and services; and
    - Adapting access rights of users who have changed roles or jobs and periodically reviewing access rights with owners of the information systems or services.
  - The allocation and use of privileged access rights should be restricted and controlled;

- Access to information and application system functions should be restricted in accordance with the Organization's access control policy;
- Enable Single Sign-On (SSO) - By using SSO you will provide your users the ability of use the same set of credentials to sign-in and access the resources that they need, regardless where this resource is located; and
- Use role based access control - Restricting access based on the need to know and least privilege security principles is imperative for organizations that want to enforce security policies for data access.

➢ **Identity Management for Customers IDs**

- A formal customer ID creation process shall be documented and implemented to enable customers to create an account with e-commerce merchants;
- Each customer shall have a unique user ID assigned to them that shall be protected with a strong password;
- Organization's shall provide Level of Assurance – 2 of ISO/IEC DIS 29115 for User Registration;
- Organizations shall ensure that the customers shall be issued a single ID which should be linked with a personal identifier such as but not limited to mobile phone number, email ID etc.;
- Organizations shall provide option to customers to link their login ID with their Facebook, Google or any other social media account;
- Organizations shall periodically review customer IDs and all the dormant IDs shall be disabled/ removed; and
- Enforce multi-factor authentication (MFA) for customers.

3.3 Payment Confirmation

➢ **Security Controls for Payment Instruments**

- Cards (Credit and Debit): Credit and debit cards are widely used for ecommerce transactions. The following guidelines shall be referred to enhance security of payments through cards:
  - o Ecommerce merchants shall select the right acquirer/ payment processor and service provider(s). They shall partner with an acquirer/payment processor that can provide effective risk management support and demonstrate a thorough understanding of Internet fraud risk and liability;
  - o Focus on risk reduction: capture only essential card and cardholder details by highlighting required transaction data fields and verifying the card and customer data that is received through the Internet;
  - o Build internal fraud prevention: build a risk management infrastructure, robust internal fraud avoidance files, and intelligent transaction controls;
  - o Apply fraud screening: Fraud-screening methods can help minimize fraud for large-purchase amounts and for high-risk transactions. By screening online card transactions carefully, organizations can avoid fraud activity before it results in a loss for business;
  - o Organizations shall encrypt all the card holder details that are being stored;
  - o Organizations shall not store Card Verification Number (CVV) of cardholders;

- Implement 3D Secure (Verified by Visa or Securecode by Mastercard) or any other leading industry standard to ensure security for transactions;
- Protect the merchant account from intrusion: Using sophisticated computers and high-tech tools, cyber-attackers are gaining access to shopping cart and payment gateway processor systems, attacking vulnerable e-commerce merchant accounts, and making fraudulent merchant deposits. By taking proactive measures, organizations can effectively minimize these cyber-attacks and their associated fraud risks;
- Create a secure process for routing authorizations: Before accepting any cards for online payment, ensure that there is a secure and efficient process in place to submit authorization requests through the Internet; and
- Organizations must safeguard cardholder data through PCI DSS compliance, QCB Guidelines or any other leading industry standards; and
- Multifactor Authentication or Level of Authentication – 3 of ISO/IEC DIS 29115 and above shall deployed for transactions.

- **Digital Wallets and Prepaid Payment instruments**
  - Organizations shall conduct periodic security reviews of the application and its corresponding infrastructure to identify any inherent risks;
  - A mobile application assessment shall be performed periodically to identify the associated vulnerabilities and risks associated with them;
  - These vulnerabilities should be communicated to all the stakeholders and a closure plan with timelines shall be defined for the closure of the same;
  - Organizations shall identify applicable legal and regulatory requirements and ensure compliance to the same;
  - Regulator;
  - The organizations shall ensure an annual security review of e-wallets is conducted for the following controls but not limited to the below:
    i. IT General Controls (Change Management, User Access Management, Incident and Problem Management, Patch Management and Log Management);
    ii. Business Process Controls (Organizational Policies and Procedures etc.);
    iii. Application(Web and Mobile) Security Assessment;
    iv. Security Configuration Review;
    v. Infrastructure Security Review; and
    vi. Compliance with any International Standard such as NIST Cybersecurity Framework, TCG Framework.
  - Data privacy requirements shall be considered and embedded to ensure customer’s data privacy; and
  - Organizations shall conduct security configuration reviews based on the QCERT/ NIST guidelines for network devices to identify vulnerabilities and associated risks. Further, these vulnerabilities shall be prioritized basis the severity and the closure shall be ensured within the defined timelines.

- **Online Banking e-Payments (OBeP)**
  - The banking institutions shall build a robust IT infrastructure and comply with QCB requirements;

- o Banking institutions shall deploy multi factor authentication mechanisms for authenticating consumers;
- o Banking institutions should deploy a fraud monitoring solution as a safeguard against online financial frauds;
- o It is recommended that organizations should define a robust cybersecurity framework and conduct periodic assessments to ensure compliance to the established policies and procedures;
- o All the high risks transactions shall be monitored and the notifications shall be sent to the customers through SMS/email; and
- o A financial institution's board and management should understand the risks associated with e-banking services and evaluate the resulting risk. Banks should respond to these risks by having a clear strategy driven from the top and should ensure that this strategy takes account of the effects of e-banking, wherever relevant. Such a strategy should be clearly disseminated across the business, and supported by a clear business plan with an effective means of monitoring performance against it.

- **Cash on Delivery**
  - o Cash security needs to be implemented and followed by all staff and management to the letter;
  - o Geographical zoning shall be done while providing cash payment option to the customers;
  - o Third party contracts outlining the terms and conditions of the services with logistics partners shall be in place. The contracts shall clearly define the service level agreements; and
  - o The ecommerce merchant shall periodically monitor the agreed service level agreements with the logistics service provider and the stakeholders shall be kept informed.
- **Secure Payment Practices for Customers**
  - o Memorize the PIN and e-banking passwords as they are personal information. Do not write PIN or e-banking passwords down;
  - o Do not share PIN and e-banking information with anyone;
  - o Update your banking/personal information directly in the bank's branch;
  - o Call the bank immediately in case:
  - o Payment card is lost; or
  - o A suspicious transaction.
  - o Keep all receipts and transaction records;
  - o Change online banking passwords regularly;
  - o Review bank account transactions regularly to identify any suspicious transactions;
  - o Research the merchant before placing an order: Always buy from reputable stores and resellers websites;
  - o Check the amount before placing the order;
  - o Site spoofing - Websites that appear professionally designed and legitimate with the purpose of collecting sensitive information from unsuspecting visitors. These website can be detected by carefully checking the URL;

  - Never respond to or open internet links or attachments in unsolicited emails;
  - Shop at secure websites: A secure website uses encryption technology to transfer information from computer to online merchant's computer system which keeps confidential information such as credit card details etc. safe;
  - Look for "Https" in the web address or URL (when entering personal information). This implies that the information is encrypted between the browser and the merchant's, which keeps it safe from unauthorised access;
  - Don't let sites store credit card information on file;
  - Making sure there is a tiny closed padlock in the address bar, or on the lower right corner of the window;
  - Always check for the browser "lock" icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate Web site;
  - Install and keep the security software (firewall, antivirus and anti-spyware software) up to date: It's important to install and keep such softwares up to-date, and perform regular scans of computer to help protect from threats as viruses, spyware, spam and generally safeguard personal information;
  - Keep system and web browser software up to date;
  - Use personal devices and private Wi-Fi for online shopping rather than a public computer and Wi-Fi;
  - Make sure to logout from the shopping website; and
  - Do not disclose online payment and shopping passwords.

3.4 Design Best Practices

- **Application Security**
  - The organization shall ensure that for all in–house developed application or applications within its use:
    - Integrity of the automatic data processing systems is maintained at all times;
    - Privacy of data is maintained; and
    - Adequate internal mechanisms are in place for reviewing, monitoring and evaluating its controls, systems, procedures and safeguards.
  - The organization shall ensure information involved in application services transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay;
  - The organization should consider following set of controls to ensure security of its applications:
    - Secure development shall be followed to build a secure service, architecture, software and system considering security of the design phase, development environment and appropriate check points in the development cycle.
    - Business application software in development shall be kept strictly separate from production application software through physically separate computer systems or separate directories or libraries with strictly enforced access controls;
    - Documentation reflecting the nature, approval and performance of all significant

changes to production computer and communications systems owned by organization shall be prepared and approved before any change takes place;

- Management shall ensure that all software development and software maintenance activities performed by in-house staff subscribe to organization's policies, standards, procedures, and systems development conventions; and
- Every non-emergency change to production systems of organization shall be shown to be consistent with the information security architecture and approved by management as part of the formal change control procedure.

- The organization shall design secure information system engineering principles at all architecture layers namely: business, data, applications and technology;
- The organization should establish acceptance criteria for new information systems and information processing facilities, upgrades and new versions and suitable tests of the systems shall be carried out during development and prior to actual production;
- Security testing shall be conducted by organizations to address vulnerabilities of Open Web Application Security Project against the security requirements identified in the planning phase and the vulnerabilities, which can be exploited by internal/ external threat source, in the modules being developed; and
- The following technical controls should be taken into controls for implementing policies for application security:
    - Ensure application is protected against unauthorised access, alteration, destruction, disclosure or dissemination of records and data;
    - Implement least privilege, restrict users to only the functionality, data and system information that is required to perform their tasks;
    - Failed authentication attempts shall be recorded in the audit log, including the date, time, user ID, and source address of the login attempt;
    - Ensure the network through which electronic means of communications are established amongst the market participants on application is secure against unauthorized entry or access;
    - Application/website has standard transmission and encryption formats amongst the market participants on the platform in order to protect the information from any disruption, hacking, etc.;
    - Implement encryption for the transmission of all sensitive information. This should include TLS for protecting the connection and may be supplemented by discrete encryption of sensitive files or non-HTTP based connections;
    - TLS certificates should be valid and have the correct domain name, not be expired, and be installed with intermediate certificates when required;
    - All cryptographic functions used to protect secrets from the application user must be implemented on a trusted system (e.g., The server);
    - Application/website has established adequate procedures and facilities to ensure that it is protected against loss or destruction and arrangements have been made for disaster recovery at a location different from the existing place;
    - Application/website has Management information system supporting internet based e-commerce business operations in order to realize a real-time connection with e-commerce core systems and of ensuring effective isolation between other application systems, avoiding the external transmission and spread of information security risks
    - Application/website has robust firewall, intrusion detection, data encryption, disaster recovery and other internet information security management systems;

- Application/website has means available to ensure that the information displayed on the webs-site, the processes, procedures and any other mechanism by whatever name called, displayed and implemented on the platform are available at all times for verification and scrutiny;
- Provide a method for users to log out of the application. Logging out should clear all session state and remove or invalidate any residual cookies;
- Use a cryptographically well-seeded pseudo-random number generator to generate session tokens. Use encryption (such as SSL encrypted web pages) to protect the confidentiality and integrity of the session;
- Data received from untrusted data sources must be properly checked before first use;
- Use minimal file system permissions on all platforms. Use 'ch'-rooted jails and code access policies to restrict where the files can be obtained or saved to;
- Utilize task specific built-in APIs to conduct operating system tasks. Do not allow the application to issue commands directly to the Operating System, especially through the use of application initiated command shells;
- Use checksums or hashes to verify the integrity of interpreted code, libraries, executables, and configuration files ;
- Utilize locking to prevent multiple simultaneous requests or use a synchronization mechanism to prevent race conditions;
- Protect shared variables and resources from inappropriate concurrent access;
- Explicitly initialize all variables and other data stores, either during declaration or just before the first usage;
- Define which HTTP methods, Get or Post, the application will support and whether it will be handled differently in different pages in the application;
- Disable unnecessary HTTP methods, such as WebDAV extensions. If an extended HTTP method that supports file handling is required, utilize a well-vetted authentication mechanism;
- Review all secondary applications, third party code and libraries to determine business necessity and validate safe functionality, as these can introduce new vulnerabilities.
- Implement safe updating: If the application utilizes automatic updates, then use cryptographic signatures for code and ensure that on download clients verify those signatures. Use encrypted channels to transfer the code from the host server.

- The organization shall refer to industry best practices, OWASP top 10, QCERT guidelines, TCG guidelines etc. while designing controls to ensure security of its application.

Design Requirement

- The organizations shall evaluate the proposed design, security controls and methodology and ensure that the design integrates with the principles of information security. Information security should be considered in all aspects of software development life cycle ;
- The organization should consider various methods such as deriving compliance requirements from policies and regulations, threat modelling, incident reviews, or use of vulnerability thresholds to identify information security requirements. These requirements shall be documented and reviewed by all stakeholders;

- The organization shall analyse the security risks for any new technology and the design shall be reviewed against known attack patterns. These principles shall be reviewed at periodic intervals to ensure that they are effectively contributing to enhanced standards of security within the engineering process;
- Organizations shall develop a clear, concise statement of privacy policy and make it available to website visitors through links on the home page. This practice may be subject to legal requirements. To allay customer concerns about providing personal data, the privacy policy should define:
    - o What customer data is collected and tracked;
    - o With whom this information is shared; and
    - o How customers can opt out.
- Establish transaction data fields that can help organizations to detect risky situations, and require the customer to complete them. Certain transaction data fields can play an important role in assessing the fraud risk of a transaction. Key risk data fields include the following:
    - o Demographic information, such as telephone numbers, that can be validated using reverse directory look-ups;
    - o E-mail address, particularly when it involves an “anonymous” service.
    - o Cardholder name and billing address, which can be validated using directory look-up services;
    - o Shipping name and address, particularly if this information is different from the cardholder’s billing information; and
    - o Card Verification Value 2 (CVV2), especially for websites selling higher risk goods or services.
- It is recommended that Organizations shall screen for high-risk international addresses. Accepting transactions from certain international locations may carry high levels of risk. Capture and translate the Internet Protocol (IP) address to identify the computer network source;
- Use a geo-location software/service to determine the IP address country; and
- Match the IP address country with the billing and shipping address country. If the countries do not match, out-sort the order for further review.

➢ Integration with Social Media, Forums, Blogs

- The organizations should focus on “testing waters “ to ascertain if social media could be used as two way interactive channel to listen and engage its social media base spanning across its customers, partners, general public and employees; and
- The organizations which are focused on growing and improving social applications should take following set of controls into consideration :
    - o Define Social media strategy which includes: Strategy and vision definition, governance model, social media maturity assessment, sentiment and influencer analysis etc.;
    - o The organizations should identify and assign individuals or departments within the organization to monitor social media channels in isolated pockets;
    - o Conduct routine audit for risk evaluations and privacy considerations.
    - o Measure, monitor, analyse and improve social performance indicators to establish greater operational efficiencies.
- It is recommended that the organizations shall Search engine optimization and Search engine marketing to enhance the websites visibility.

- **Product Ratings**
  - All organizations offering products online shall bring to the prospects attention the following information, sharing prospects :
    - The type of consumer for whom the product is intended;
    - Main characteristics of the product;
    - Options and coverage provided by the product, as applicable;
    - Exclusions and limitations associated with the product, if any;
    - The total premium and other charges that the consumer shall pay (including all applicable taxes) or, if an exact amount cannot be indicated, the basis for the calculation of the amount, so that the prospects can verify it;
    - The prospects "right to cancel" if applicable, as well as the duration of the cancellation period and procedures for exercising that right;
    - State time frames for order processing and send e-mail confirmation to customers and order summary within one business day of the original order;
    - Any time limit on the validity of the information provided.

- **Content Update**
  - Whenever a software package needs to be modified the following points should be considered:
    - The risk of built-in controls and integrity processes being compromised;
    - Whether the consent of the vendor should be obtained;
    - The possibility of obtaining the required changes from the vendor as standard program updates;
    - The impact if the organization becomes responsible for the future maintenance of the software as a result of changes;
    - Compatibility with other software in use.
  - If changes are necessary the original software should be retained and the changes applied to a designated copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software;
  - All changes shall be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body; and
  - Organizations shall fully disclose to the customer on the payments page of the website, the country current operations and information about the transaction currency used for the purchase.

3.5. Accessibility

- It is recommended that the website shall support multi-language feature (such as Arabic, English etc.); and
- As a good practice, the organizations should comply with IAB standards for digital advertising.

Appendix 1:
Terms and Definitions

S.No	Term	Definition
1	Access Control	Refers to ensure that access to information assets is authorized and restricted based on business and security requirements.
2	Asset	Anything that has value to an organization
3	Attack	An attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
4	Authentication	It is the provision of assurance that a claimed characteristic of an entity is correct.
5	Authorization	Authorization is the process used to grant permissions to authenticated users. Authorization grants the user, through technology or process, the right to use the information assets and determines what type of access is allowed (read-only, create, delete, and/or modify). The system or application should determine if the user has permission to perform the requested operation.
6	Availability	It is the property of being accessible and usable upon demand by an authorized entity.
7	Confidentiality	It is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
8	Continual Improvement	It is defined as the recurring activity to enhance performance.
9	Effectiveness	It is the extent to which planned activities are realized and planned results achieved.
10	Information	Applies to any storage, communication, or receipt of knowledge, such as fact, data, opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.
11	Information Asset	Information that has value to our company including, people, paper, Logical (Information), Physical, Software and Service, Site.
12	Information Processing Facilities	Any information processing system, service or infrastructure, or the physical location housing it.
13	Information Security	It is defined as the preservation of confidentiality, integrity and availability of information.
14	Information Security Event	It is identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant.
15	Information Security Incident	Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

16	Integrity	It is the property of accuracy and completeness.
17	Risk	Combination of the likelihood of an event and its impact.
18	Threat	Threat is the potential cause of an unwanted event that may result in harm to an organization and its assets.
19	Virus	A computer virus is a piece of malicious software designed to attach itself to other programs and to replicate itself into other programs, ultimately very possibly infecting every program in a system. There is also a variant known as a macro virus, which attaches itself to the macros, which are a part of some word processor and spreadsheet programs. Other malicious software goes by such names as worms, Trojan horses or time bombs. These can all be very damaging to a system but are free standing rather than replicating attachments.
20	Vulnerability	It is a flaw or weakness in system security procedures, design, implementation, or internal controls that can be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy
21	Card Verification Value	The Card Verification Value (CVV), is a system the credit card companies are introducing to help protect against fraud. It is a code 3 digits long that is calculated from the data on the magnetic strip and cannot be forged.

Appendix 2: List of Sources

List of Sources

- ISO 27001:2013 Standard
- Identity Management - SANS Institute
- OWASP Application Security Guidelines
- Web Content Accessibility Guidelines (WCAG) 2.0
- Modern Technology and E-Banking Services Risks Annex No. (192)
- ISO/IEC DIS 29115 -- Information technology – Security techniques – Entity authentication assurance framework
- Processing e-commerce payments - Visa
- Ecommerce Payment Methods Report 2016 – The Paypers
- Mobile payment: war of the wallets, 2015 – EY
- The National Information Assurance Policy
- National ICS Security Standard
- National Cyber Security Strategy
- QCB guidelines on Banking supervision rules.

MOTC
motc.gov.qa