
# GUIDE ON BUILDING WEBSITES FOR SMEs

**Published 20 July 2016**
**Revised 10 July 2018**

TABLE OF CONTENTS

# PART 1: OVERVIEW

## 1 Introduction

1.1 Many organisations find it increasingly important to have a website as part of their sales, marketing and customer relationship management efforts. Websites typically consist of viewable content, but may also offer features like online shopping, memberships, reward programs, event registration and feedback.

1.2 As such features may require the website to collect, use, disclose, and store personal data, like customer and payment details, organisations should be aware of their obligations under the Personal Data Protection Act ("PDPA") (for more details, see Section 6).

## 2 Purpose of this Guide

2.1 This guide contains a list of useful topics for organisations to consider when building secure websites that collect, use, disclose, or store personal data.

2.2 While the list is not exhaustive, it seeks to assist organisations by providing key considerations for the process of setting up a website. It can also be used by business owners to guide their discussions with IT vendors whom they engage to build their websites.

# PART 2: SETTING UP A WEBSITE

## 3 Key Considerations

3.1 When setting up a website, organisations should consider:

- The features and functions of the website (e.g. online ordering portal, membership management, online forums);
- The types of personal data that will be collected;
- The extent of security required;
- Where the website will be hosted;
- Whether the development of the website (or parts of the website) will be outsourced;
- The maintenance of the website, and whether it will be outsourced; and
- Resiliency of the website (Business continuity requirements)

3.2 As websites are constantly connected to the Internet, they are subjected to a multitude of cyber threats that may compromise the website and expose any personal data it collects. Data breaches can be costly to the organisation as it may lead to financial loss and cause consumers to lose trust in the organisation.

3.3 Organisations should thus ensure that the protection of the personal data and the security of the website is a key design consideration at each stage of the website's life cycle. This cycle typically includes requirements gathering, design & development, user acceptance testing, deployment and operations & support.

3.4 Of note, where data protection is not considered until the development of the website has been completed, making changes to the website at that later stage can add more cost to the organisation including cost incurred to resolve any security breaches.

## 4 Outsourcing

4.1 The setting up of a website, particularly with more complex functions such as online ordering, membership management and event management, requires IT expertise. As not all organisations have the resources to develop such websites by themselves, they may decide to outsource the development and maintenance of the website. This would entail the engagement of one or more IT vendors to:

- Provide the design, layout and artwork/graphics for the website;
- Develop (program) the website to perform the intended functions;
- Host the website so that it is accessible on the Internet;
- Install security features to ensure security requirements are met;
- Perform administrative tasks like managing user accounts; and/or
- Maintain the website by updating the design, layout, graphics and programming when required.

This section describes general considerations that organisations should be aware of when engaging IT vendors to set up websites.

### 4.2 Negotiating IT Vendor's Responsibilities

4.2.1 Organisations should emphasise the need for personal data protection to their IT vendors, by making it part of their contractual terms. The contract should also state clearly the responsibilities of the IT vendor with respect to the PDPA. When discussing the scope of the outsourced work, organisations should consider whether the IT vendor's scope of work will include any of the following:

- Requiring that IT vendors consider how the personal data should be handled as part of the design and layout of the website.
- Planning and developing the website in a way that ensures that it does not contain any web application vulnerabilities that could expose the personal data of individuals collected, stored or accessed via the website through the Internet.
- Requiring that IT vendors who provide hosting for the website should ensure that the servers and networks are securely configured and adequately protected against unauthorised access.

- Requiring IT vendors to ensure that all work done is fully documented and that all documentation is handed over to the organisation at the completion of the project. Documents should capture the website's requirements, design specifications, user test scripts, user test results, as well as server and network configurations.
- When engaging IT vendors to provide maintenance and/or administrative support for the website, requiring that any changes they make to the website do not contain vulnerabilities that could expose the personal data. Additionally, discussing whether they have technical and/or non-technical processes in place to prevent the personal data from being exposed accidentally or otherwise.
- Requiring that IT vendors providing maintenance and/or administrative support to ensure that all changes to the website are secure and documented, and that the documentation is kept up to date.

### 4.3 Confidentiality

4.3.1 An organisation should make clear the purposes for which its IT vendor is engaged. Organisations should require that IT vendor(s) ensure that the personal data of individuals handled by the website is not disclosed to unauthorised parties by their personnel or sub-contractors.

4.3.2 IT vendors should have processes in place for the secure handling of the personal data during the development and especially maintenance phases. As a good practice, IT vendors should also inform organisations of all sub-contractors and their assigned responsibilities.

4.3.3 Confidentiality agreements may also be signed by all personnel and sub-contractors who have access to the personal data handled by the website.

4.3.4 Where possible, technical measures should be implemented to ensure consistent enforcement of the confidentiality requirements. Organisations may also wish to consider using encryption and/or data masking measures.

### 4.4 Ready-Made Software/Software Components

4.4.1 Organisations and IT vendors may choose to use ready-made software/software components from third parties who are not involved with the development of the website. While using ready-made software/software components may speed up the programming of the organisation's website, organisations and their IT vendors should have a clear understanding of how such ready-made software/software components handle personal data and how it must be configured, before utilising it for their website.

4.4.2 Please refer to the "ICT Outsourcing" section in PDPC's "Guide to Securing Personal Data in Electronic Medium", for more information on the use of ready-made software/software components.

# PART 3: WEBSITE SECURITY

## 5 Security Policies and Processes

5.1 Security arrangements for the organisation's website should not be limited to technical solutions only. Organisations should also put in place policies and processes to protect the personal data collected, stored or accessed through their website.

5.2 There should be processes where vendors have to get approval from organisation to make changes to the website. Some suggested policies and processes are described in this section, for organisations and their IT vendors (if any) to consider for implementation.

5.3 Organisations may also require that their IT vendor(s) propose more detailed IT policies based on the suggestions in this section.

### 5.4 Risk Management

5.4.1 Organisations should conduct a risk assessment of the website, or require that their IT vendor(s) conduct one or assist the organisation in its assessment. A risk assessment will help to identify the security risks that the website faces, and to identify the possible impacts to the organisation, if the personal data was exposed.

5.4.2 Based on the risk assessment, the organisation, with the help of their IT vendor (if any), will be able to better select the most appropriate security measures for the website.

5.4.3 The risk assessment and security arrangements should be reviewed and updated on a regular basis

### 5.5 Security Configuration Management

5.5.1 Organisations should ensure, or require their vendor(s) to ensure, that the software and hardware components of the organisation's website are properly configured to prevent unauthorised access. This includes reviewing operating systems, checking if appropriate antivirus/anti-malware software are in place and setting firewall rules to only allow authorised traffic. The configuration of each component should also be fully documented, kept up to date, and reviewed regularly.

5.5.2 There should also be a plan for testing and applying patches and updates for the website's software and hardware components. This includes having a process and person responsible to monitor new patches and updates that become available.

## 5.6 Security Testing

5.6.1 Testing the website for security vulnerabilities is an important aspect of ensuring the security of the website. Penetration testing or vulnerability assessments should be conducted prior to making the website accessible to the public, as well as on a periodical basis (e.g. annually). Any discovered vulnerabilities should be reviewed and promptly fixed to prevent data breaches.

5.6.2 Where organisations have outsourced the development of its website, they should either require the IT vendor(s) to conduct the above security testing, or arrange for a cybersecurity vendor to do so. As a baseline, organisations may wish to consider using the Open Web Application Security Project (OWASP) Testing Guide and the OWASP Application Security Verification Standard (ASVS) to verify that security requirements for the website have been met.

## 5.7 Personal Data Inventory

5.7.1 Organisations and any engaged IT vendors should keep track of where the collected personal data is stored, and should impose a limit on how long the data is kept, or regularly review their need to continue storing the personal data.

5.7.2 If the personal data is no longer required, organisations and any engaged IT vendors should then ensure that the personal data is anonymised or disposed of in such a way that it cannot be recovered.

## 5.8 Incident Management

5.8.1 Organisations and any engaged IT vendors should plan their potential actions in the event that the website's security is compromised.

5.8.2 An incident response plan that is prepared in advance will be useful for handling security incidents to ensure that security breaches are immediately dealt with to prevent personal data from being exposed.

5.8.3 The incident management plan should cover business continuity requirements such as back-up, restoration and where applicable, preservation of evidence for investigation. Additionally, organisations should clarify the roles between themselves and their IT vendor(s) on incident management.

# 6 Security Design

6.1 Organisations should require its IT vendor(s) to include security as an important requirement when designing the website. Some key security requirements are described in this section.

## 6.2 Access Control

6.2.1 Access control is a critical part of the website's security arrangements. An effective access control scheme should be designed such that:

- Only authorised users (usually staff of the organisation) are allowed to access the website's administrative functions and personal data handled by the website. This is usually achieved by requiring the user to login using a user ID and password, two-factor authentication (2FA) methods are recommended for added security. User IDs and passwords should be unique to each user, and should not be shared;
- All users should only be able to see the website functions and data that they are allowed to access. For example, members of the public should not be allowed to access the website's administrative functions, but can view and edit their own membership profile;
- The list of users who have access to the administrative functions should be reviewed and updated regularly to ensure that each user has valid reasons to access the functions and data they are assigned. For example, staff members who have resigned, been transferred, or who had a change in job scope may need their website access updated or removed;
- Only passwords with sufficient length and complexity are allowed. For example, passwords of at least 8 characters, and containing at least 1 upper case character, number and symbol. At the same time, the system can provide tips to users on strong passwords, when asking the user to create a password. Such tips may include :
    - Using a five different words that relate to a memory that is unique to the user e.g. Learnttorideabikeatfive
    - Including uppercase and lowercase letters, as well as numbers and symbols e.g. LearnttoRIDEabikeat5!
    - Not using easily derivable personal information such as names, birthdays and phone numbers in the password
    - Not using a password that is already being used in another system
- Users are prevented from accessing the website if they enter incorrect IDs or passwords several times in a row. For example, users who have entered their passwords incorrectly more than 6 times will not be allowed to log in, and would need to be re-verified to unlock their user account;

- Users are required to change their passwords regularly. For example, users can be asked to change their password every 90 days;
- Passwords are encrypted during transmission and encrypted or hashed in storage. For example, the login page should use HTTPS, and the password is hashed before being saved in the database;
- User accounts which have not been used for a prolonged period [i.e. dormant], are suspended. For example, users who have not logged in during that period would not be able to access the website until their account is reactivated.

## 6.3 Audit Log

6.3.1 Audit logs record the events experienced by the website, including the actions of the users. Logs are important for determining the cause of security incidents, as well as for monitoring the overall health of the website. Examples of audit logs include web logs, server logs and application logs.

6.3.2 The logs of the website should be designed to record computer or user events, together with the respective time stamp, such as:

- System events like start-up, shutdown
- Security events like access violations
- User logins and logouts, including unsuccessful login attempts
- Actions performed by users

6.3.3 As audit logs take up storage space and will increase in size over time, organisations should decide (together with their IT vendors) on the necessary actions and events that should be recorded. Additionally, the system should be designed such that the audit logs cannot be modified.

6.3.4 The website's audit logs should be regularly reviewed, to ensure that there has not been any unauthorised activity. If such activity is detected, then the organisation should apply their incident plan to investigate and retain evidence and take remedial actions to prevent further occurrences. Organisations who engage external IT vendors should discuss how this review can be carried out, by whom and the frequency.

## 6.4 Server and Network Security

6.4.1 Websites require servers and networks in order to function and be accessible from the Internet. Some measures for securing servers and networks include:

- Installing application control[1] and up-to-date antivirus/anti-malware software on the servers
- Deploying firewalls and/or intrusion detection systems on the network
- Implementing HTTPS for all pages that accept user input. For example, member registration, user login, event registration.

### 6.5 Website Programming

6.5.1 When programming the website, programmers should be aware of the common website vulnerabilities, and adopt the proper programming techniques and practices to avoid them. Programmers can use the OWASP Top 10 vulnerabilities list as guide and some common vulnerabilities include:

- Injection (e.g. SQL Injection)
- Cross-site scripting
- Buffer overflows
- Poor authentication & session management

6.5.2 Organisations and any engaged IT vendors should ensure that personal data cannot be exposed, either accidently or by design, through any such vulnerabilities. The website functions should be thoroughly tested or scanned for vulnerabilities, before the website is launched.

6.5.3 Organisations should discuss with their external IT vendors on whether vulnerability scanning is included in their scope of work or procured from another service provider.

## 7 PDPA Obligations

7.1 Section 24 of the PDPA requires an organisation to make "reasonable security arrangements to protect personal data in its possession or under its control to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks."

7.2 If the website is hosted overseas and personal data of individuals are transferred from Singapore to the overseas destination, then organisations are required to comply with Section 26 of the PDPA, which sets out the requirements to be met for the transfer of personal data outside Singapore.

7.3 IT vendors who have access to the personal data for the purpose of hosting or maintaining the website, may be considered data intermediaries under the PDPA. Under Section 4(2), data intermediaries are required to comply with Sections 24 (which is mentioned above) as well as Section 25, which requires organisations to cease

[1] Application Control allows only authorised applications to work and reduces the risk of unauthorised applications such as malware from affecting the system.

retention of personal data where the purpose of the data is no longer necessary for legal or business purposes or where the purpose of the data is no longer served by its retention.

7.4 Additionally, organisations should note that they may be held liable for the actions or omissions of its data intermediary that amounts to a breach of a Data Protection Provision. The organisation should therefore ensure that its contract with its data intermediary imposes sufficient obligations on the data intermediary to ensure the organisation's own compliance with the PDPA.

## 8 Additional Resources

8.1 Organisations and IT vendors are encouraged to refer to the following resources on the PDPC website, which provide more information on the areas that are mentioned briefly in this guide. For general cybersecurity tips and resources, organisations can visit the Gosafeonline website (https://www.csa.gov.sg/gosafeonline).

8.2 Advisory Guidelines (https://www.pdpc.gov.sg/ag)

i) Chapter 17 (The Protection Obligation) of the Advisory Guidelines on Key Concepts in the PDPA

ii) Chapter 18 (The Retention Limitation Obligation) of the Advisory Guidelines on Key Concepts in the PDPA

iii) Chapter 19 (The Transfer Obligation) of the Advisory Guidelines on Key Concepts in the PDPA

iv) Chapter 7 (Online Activities) of the Advisory Guidelines on the Personal Data Protection Act for Selected Topics

8.3 Other Guides (https://www.pdpc.gov.sg/og)

i) Guide to Securing Personal Data in Electronic Medium

ii) Guide to Managing Data Breaches

END OF DOCUMENT

BROUGHT TO YOU BY


IN PARTNERSHIP WITH