IT RISK ASSESSMENT POLICY TEMPLATE

IT RISK ASSESSMENT POLICY

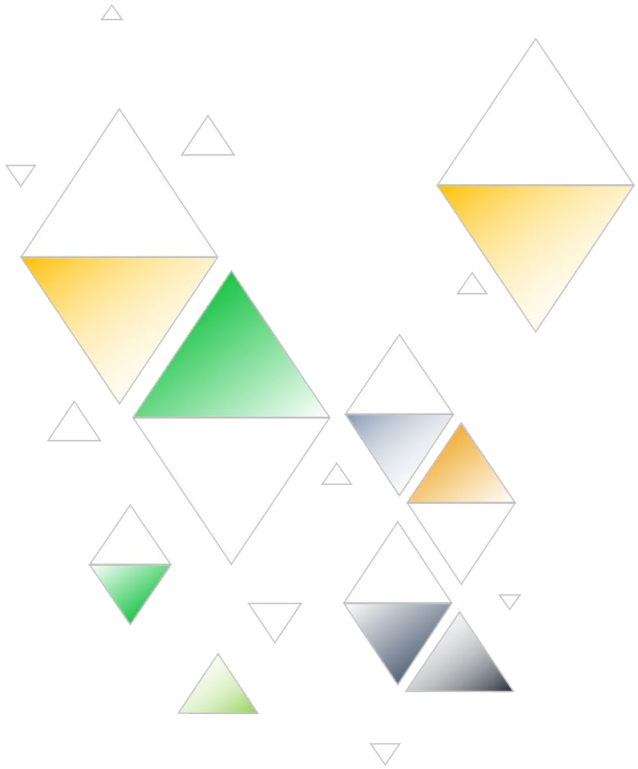
PROJECT NAME

ADDRESS

WEB ADDRESS

VERSION 0.0.0

MM/DD/YY



PREPARED BY		**DATE**	
REVIEWED BY		**DATE**	
APPROVED BY		**DATE**	

POLICY DETAILS

POLICY NAME				**POLICY NO.**	
EFFECTIVE DATE		**DATE OF LAST REVISION**		**VERSION NO.**	
ADMINISTRATOR RESPONSIBLE		**CONTACT INFORMATION**			
APPLIES TO apply group names to define applicable areas of staff					
GROUP 1		GROUP 2		GROUP 3	
GROUP 4		GROUP 5		GROUP 6	

VERSION HISTORY

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**

TABLE OF CONTENTS

INTRODUCTION

Describe the purpose of the policies and procedures.

SCOPE

Specify to whom these policies and procedures apply, such as all employees, or employees, visitors, and contractors.

TECHNOLOGY HARDWARE PURCHASING POLICY

PURPOSE OF THE POLICY

Detail guidelines for the purchase of hardware for the business to ensure that all hardware is appropriate.

PROCEDURES

PURCHASE OF HARDWARE

Describe the policy for the purchase of all desktops, servers, laptops, tablets, computer peripherals and mobile devices, and other hardware. Describe any minimum capabilities or versions, compulsory brands, and details such as whether tethered mouse devices are permitted.

Describe how warranties are retained and any purchasing procedures noted in other documents.

DESKTOPS, LAPTOPS, AND TABLETS
- Item 1
- Item 2

SERVERS
- Item 1
- Item 2

MOBILE TELEPHONES
- Item 1
- Item 2

COMPUTER PERIPHERALS
- Item 1
- Item 2

SOFTWARE PURCHASES POLICY

PURPOSE OF THE POLICY

Describe the aim of the software policy and whether it applies to single licenses, bundles, and so on.

PROCEDURES

REQUEST FOR SOFTWARE

Describe how a request for software is made.

PURCHASE OF SOFTWARE

Describe who is allowed to purchase software and any preferred product vendors. Also describe characteristics, such as version numbers.

OBTAINING OPEN SOURCE OR FREEWARE SOFTWARE

Add any guidelines for downloading and installing open source software.

POLICY FOR USE OF SOFTWARE

PURPOSE OF THE POLICY

This policy provides guidelines for the use of software for all employees within the business to ensure that all software use is appropriate. Under this policy, the use of all open source and freeware software will be conducted under the same procedures outlined for commercial software.

PROCEDURES

SOFTWARE LICENSING

Describe guidelines for licensing use.

SOFTWARE INSTALLATION

Describe who is responsible for installation and registration of software.

SOFTWARE USAGE

Describe limits of software use and what is considered inappropriate use. If employees are prohibited from installing their own software on work equipment, explain this here.

BREACH OF POLICY

Describe any actions and consequence for breach of software policy.

BRING YOUR OWN DEVICE (BYOD) POLICY

PURPOSE OF THE POLICY

Describe your policy guidelines for the use of personally owned notebooks, smart phones, tablets for company purposes.

PROCEDURES

CURRENT MOBILE DEVICES APPROVED FOR COMPANY BUSINESS USE

List the personally owned mobile devices that are approved for company use:

Add the type, make and model of approved device.

REGISTRATION

Detail the registration process for personal devices.
List approved business purposes. Examples include business email messages, business calls, and approved product apps.

- Purpose 1
- Purpose 2
- Purpose 3

Describe conditions for using personal devices for business purposes. Conditions may include not transmitting sensitive information, to ensure information is backed up on another device, to guard the device against compromise in public places and on public Wi-Fi systems, and not to allow unauthorized individuals to use the device.

COMPANY RIGHTS

Describe the extent of company control and rights to intellectual property and data created on the device. For example, your company may assert its right to own all intellectual property created on the device and to delete data if the device is ever stolen or when the employee is terminated for whatever reason. Consult your CIO and legal counsel for more information.

SECURITY MEASURES FOR MOBILE DEVICES

Detail expectations for keeping devices secure.

EXEMPTIONS

Describe any exemptions.

BREACH OF POLICY

Describe any actions and consequence for breach of software policy.

INDEMNITY

Describe how employees are expected to indemnify your company in the event that illegal activity is conducted using company assets. Consult your legal advisor for more information.

INFORMATION TECHNOLOGY SECURITY POLICY

PURPOSE OF THE POLICY

Describe the aim of the security policy as it applies to IT assets and resources.

PROCEDURES

PHYSICAL SECURITY

Detail environmental and physical security measures.

INFORMATION SECURITY

Describe backup, password protection, authorization, and other measures for information security. Use a table to list individuals and security responsibilities.

TECHNOLOGY	RESPONSIBLE PERSONS

INFORMATION TECHNOLOGY ADMINISTRATION POLICY

PURPOSE OF THE POLICY

Describe your IT administration policy.

PROCEDURES

Describe administration procedures, such as listing every physical and software asset, applicable licenses, renewal dates, service agreements, and warranties.

WEBSITE POLICY

PURPOSE OF THE POLICY

Describe guidelines for the maintenance of the company website.

PROCEDURES

WEBSITE CONTENT

Detail guidelines for company website content, who is responsible, scope of content, reviewers and approvers, branding guidelines, and data privacy guidelines. Note any regulations pertinent to your website content and privacy.

WEBSITE REGISTER

Note information relevant to your domain name, such as all registered names, dates of renewal, and hosting service providers.

IT SERVICE AGREEMENTS POLICY

PURPOSE OF THE POLICY

Describe service agreements and prerequisites for signing such agreements. Include any requirements for legal review and steps in the event of problems.

EMERGENCY MANAGEMENT OF INFORMATION TECHNOLOGY

PURPOSE OF THE POLICY

Describe guidelines for emergency management of all information technology within the company.

PROCEDURES

Describe who is responsible for managing issues for hardware failures, malware, information breaches, or website disruptions, and steps for managing each type of event.

DISCLAIMER

Any articles, templates, or information provided by Smartsheet on the website are for reference only. While we strive to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the website or the information, articles, templates, or related graphics contained on the website. Any reliance you place on such information is therefore strictly at your own risk.