Parshotam & Associates

IT Risk Assessment

&

IT Security Policy

M/s Parshotam& Associates
Chartered Accountants
info@parshotamandassociates.com
+91-92045-00007

Document Information

DOCUMENT CREATION DATE:	21.10.2018		
CLASSIFICATION	○ Public	● Internal	○ Confidential
REVISION HISTORY	01.12.2019 30.06.2020		

Document Distribution List

This table serves the purpose to record and track the document distribution.

Date	Name	Purpose
	All personnel	For Information

Table of Contents

IT Risk Assessment

Brief Summary

Need of Risk Assessment

In an interdependent, fast-moving world, organizations are increasingly confronted by risks that are complex in nature and global in consequence. Such risks can be difficult to anticipate and respond to, even for the most seasoned business leaders

What can we do to make our company more resilient to significant and unpredictable risks?

Businesses all over have priorities based on their own position compared with the market as well as the market itself. Attention is normally focused onto the areas that the company perceives to have a higher business risk. However this is not so well structured and very often, business risks are not properly visualized or understood, especially as there is a lack of formality in understanding them. There is also a danger of not realizing which are the greatest risks and which of them must be focused upon by the organization. In order to improve business decision making, Risk Management today is rapidly gaining acceptance and is helping organization manage their businesses better, which in today's hypercompetitive environment is an imperative.

Organizations that succeed do so because they are best able to optimize the risk and reward equation for both strategic and Operational issues.

Organization Overview

Organization Name	Parshotam and Associates
Address	10 B, Udham Singh Nagar, Civil Lines, Ludhiana-141001 INDIA
Contact Person	Mr Nipan Bansal (Data Owner) Mr. Ravi Chopra (IS Auditor)
Telephone Number	+91-9204500007

Overview of IT system of Parshotam & Associates

S.No.	Data Required	Details
1	**Organization Name**	M/s Parshotam and Associates
2	**Organization Structure**	M/s Parshotam and Associates is a CA firm based in Ludhiana with several branch offices across the country. We have a team of 35 professionals working in different areas of business support services.
3	**Objective**	The assessment is performed with the objective to find existing of major Information technology related vulnerabilities in organization to create a secure and authentic working environment.
4	**Address of Head office**	10 B, Udham Singh Nagar, Civil Lines, Ludhiana-141001 India
5	**Overall Staff**	We are a team of 35 members in all the branches
6	**Scope**	Access Control Asset Management Awareness and Training Data Security End Point Security Network Security Vulnerability Management
7	**Policies and Procedures**	Organization policies and procedures are documented separately
8	**Current IT Controls**	Proper Antiviruses & Office Securities are installed in organization. Access control management is implemented in a way that an employee can access the only for which is authorised. CCTV are also installed for security purposes.
9	**IT Architecture**	ISP Details - Bharti Airtel Ltd.

		Asset Register
		Below listed devices are working in LAN Connectivity
		1. Desktop - 12
		2. Laptops – 10
		3. Printers – 2
		4. Landline Phone – 2
		Software Details
		1. Tally ERP 9
		2. Smart Tax
		3. Smart GST
		4. Busy Accounting software
		Network Devices – 2
		Cloud Service Provider - Google Drive
		Backup Strategy - Backup for all data is taken once in a fifteen days period and saved in Cloud.
		Anti-Malware in use – Kaspersky Small Office Security

The Methodology & Process:

In a Risk Management Context understanding of M/s Parshotam & Associates was done through:

- Identifying company's strategic objectives, stakeholder obligations, statutory requirements and the environment in which the Firm operates.
- Identifying activities, resources and assets that support the delivery of their product and services.
- Identifying and evaluating perceived risks (threats and vulnerabilities) that could have a negative impact on the organization's ability to achieve their strategic objectives.
- Assessing the management controls and its impact to mitigate the risks provides us with information on where further management attention needs to be focused.

Business Risk Assessment was carried out by the Top Management Team of Parshotam & Associates

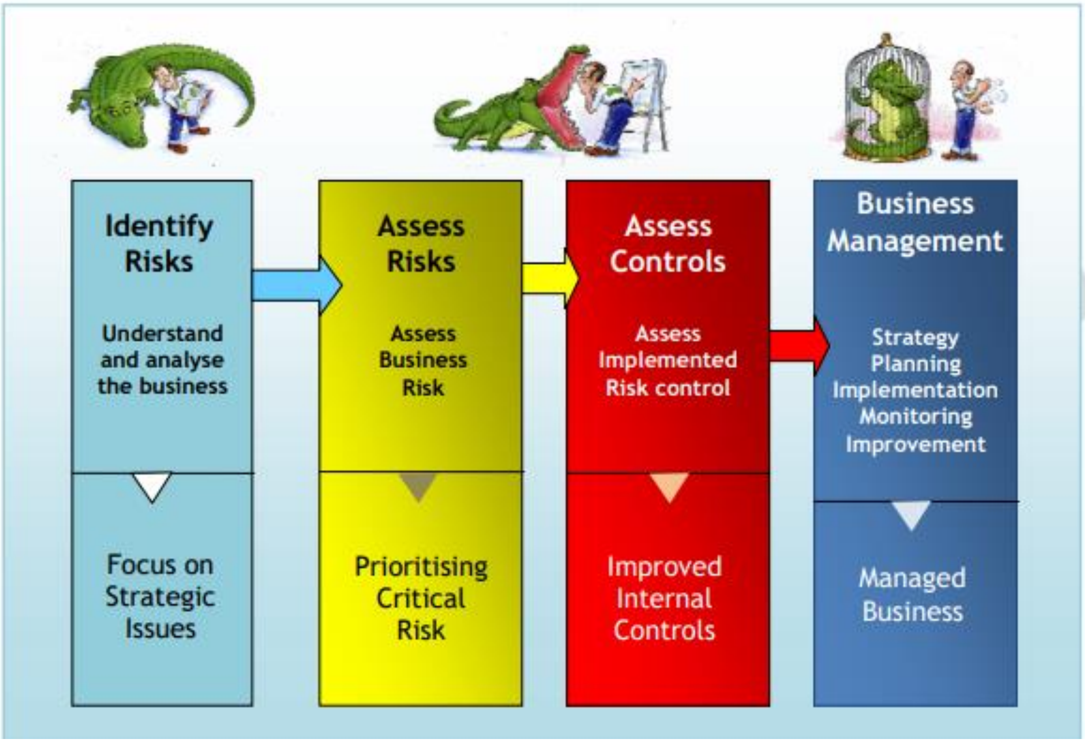
Name of Participant	Designation	Function/Designation
Nipan Bansal	Managing Partner	Administration, Monitoring & Policy Making
Ravi Chopra	Partner	Senior Partner engaged in Policies formation & Management
Manmohan Dhiman	Partner	Working Partner working in core functions of organization
Tishu Garg	Partner	Working Partner working in core functions of organization
Gurdeep Singh	Office In charge	Overall Office administration in Organization
Rishab Goyal	Manager	Working in organization's key business activities
Abhinav Garg	Intern	Assisted in Risk Assessment

This team identified the various Risks (threats and vulnerabilities) associated with its business (Activities/ Processes, Resources and Assets) in particular the effect of the uncertainty on the business objectives. The process involved a structured brainstorming. The list was screened by the group to club together similar risks. The next step involved taking the consensus of all the participants and agreed on a selected number of identified risks to be evaluated in depth.

These business risks were clearly displayed to the participants and subsequently these Risks (threats and vulnerabilities) were assessed by the Team with respect to:

- Likelihood of occurrence of the Risk
- Consequence the Risk has on the Organization

Risk Assessment Process


Identify Risks
Understand and analyse the business
Focus on Strategic Issues
Assess Risks
Assess Business Risk
Prioritising Critical Risk
Assess Controls
Assess Implemented Risk control
Improved Internal Controls
Business Management
Strategy Planning Implementation Monitoring Improvement
Managed Business

Risk(Threats & Vulnerabilities) Identification:

Identification of the business risks as perceived by the operational level team was carried out using structured brainstorming. Risks were identified w.r.t to each Strategic Business Objective.

Through the structured brainstorming session, the participants identified a comprehensive list of Risks in the business. The next step was to consolidate the common and similar risks as well as remove the duplicate ones. A rapid risk assessment based on consensus was carried out with the team to identify those risks which are crucial.

This process is a consensus process and we arrived at a list of various Business Risks (threats and vulnerabilities) as detailed herein below which were subject to a detailed analysis and evaluation.

Detailed Assessment

1. Introduction

Purpose

To empower Information Security to perform periodic Information security risk assessments for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

Scope of this risk assessment

Risk assessments can be conducted on any entity within Parshotam & Associates or any outside entity that has signed a Third Party Agreement with M/s Parshotam & Associates. Risk Assessments can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

Risk Assessment Execution

The execution, development and implementation of remediation programs is the joint responsibility of Information Security and the department responsible for the systems areas being assessed. Employees are expected to cooperate fully with any Risk Assessment being conducted on systems for which they are held accountable. Employees are further expected to work with the Information Security Risk Assessment Team in the development of a remediation plan.

Participants

Role	Participant
System Owner	Nipan Bansal
System Custodian	Ravi Chopra
Security Administrator	Ravi Chopra
Database Administrator	Manmohan Dhiman
Network Manager	Gurdeep Singh

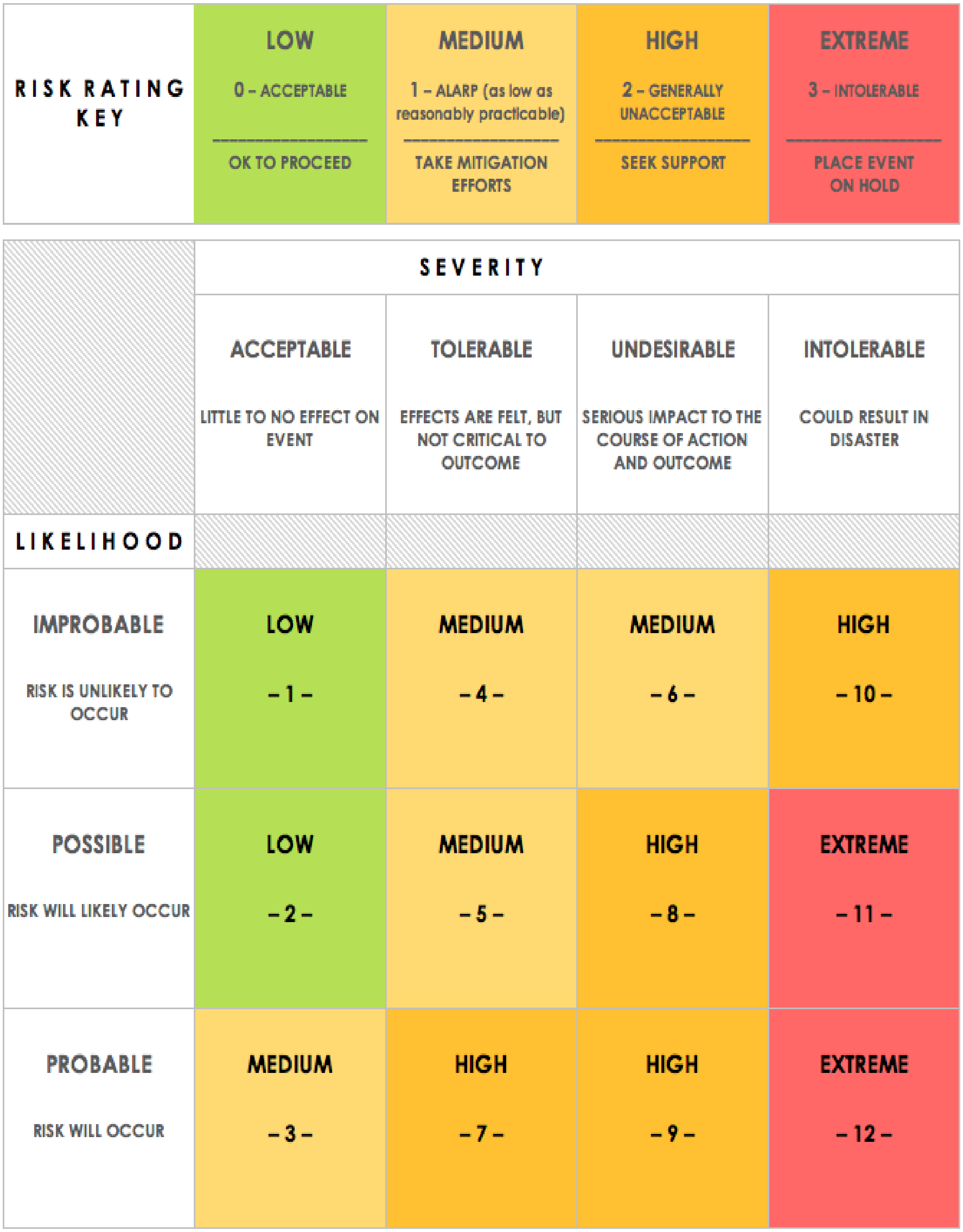
Risk Assessment team

Name of Participant	Designation	Function/Designation
Nipan Bansal	Managing Partner	Administration, Monitoring & Policy Making
Ravi Chopra	Partner	Senior Partner engaged in Policies formation & Management
Manmohan Dhiman	Partner	Working Partner working in core functions of organization
Tishu Garg	Partner	Working Partner working in core functions of organization
Gurdeep Singh	Office In charge	Overall Office administration in Organization
Rishab	Manager	Working in organization's key business activities
Abhinav Garg	Intern	Assisted in Risk Assessment

2. Techniques Used

Technique	Description
Questionnaires	1. What if analysis.
Surveys	2. Check lists.
Online resources	3. Fault Tree Analysis

3. Risk Rating Model



RISK RATING KEY	LOW	MEDIUM	HIGH	EXTREME
	0 – ACCEPTABLE	1 – ALARP (as low as reasonably practicable)	2 – GENERALLY UNACCEPTABLE	3 – INTOLERABLE
	-------------------	-------------------	-------------------	-------------------
	OK TO PROCEED	TAKE MITIGATION EFFORTS	SEEK SUPPORT	PLACE EVENT ON HOLD

	SEVERITY			
	ACCEPTABLE LITTLE TO NO EFFECT ON EVENT	TOLERABLE EFFECTS ARE FELT, BUT NOT CRITICAL TO OUTCOME	UNDESIRABLE SERIOUS IMPACT TO THE COURSE OF ACTION AND OUTCOME	INTOLERABLE COULD RESULT IN DISASTER
LIKELIHOOD				
IMPROBABLE RISK IS UNLIKELY TO OCCUR	LOW – 1 –	MEDIUM – 4 –	MEDIUM – 6 –	HIGH – 10 –
POSSIBLE RISK WILL LIKELY OCCUR	LOW – 2 –	MEDIUM – 5 –	HIGH – 8 –	EXTREME – 11 –
PROBABLE RISK WILL OCCUR	MEDIUM – 3 –	HIGH – 7 –	HIGH – 9 –	EXTREME – 12 –

4.System Characterization

Technology components

Component	Description
Applications	1. Tally ERP 9 2. Smart Tax& Smart TDS 3. Smart GST 4. Kaspersky Small Office Security 5. Printer & Scanner driver 6. MS Office 7. Google Chrome, Internet Explorer 8. EM Signer & DSC software
Databases	Server Machine connected through LAN
Operating Systems	Windows 7, Windows 10
Networks	LAN, Internet (WIFI)
Interconnections	Networking

Physical Location(s)

Location	Description
Admin Office	10 B, Udham Singh Nagar, Civil Lines, Ludhiana-141001 India

Data Used By System

Data	Description
Financial Data stored in the Server & the Client PC.	1. Financial Information of Clients 2. Basic ID documents of Clients 3. Credentials of various Government sites of clients. 4. Basic information of employees 5. Banking information of organization and clients. 6. Accounting & Taxation Software Back up

Users

Users	Description
Nipan Bansal	User of Executive Summary for management decisions. Not engaged in daily data processing.
Ravi Chopra	User of data processing by others and other client information own working.
Manmohan Dhiman	User of data processed by other team members and clients financial information for own working

Tishu Garg	User of information of clients for performing business activities.
Gurdeep Singh	User of Employee’s information for administration and payroll processing, user of basic information of clients for Invoice processing and receivables management.
Rishav Goyal	User of financial and non-financial of selected clients for processing of business services.
Abhinav Garg	User of GST and other financial information of clients for performing business relating to GST consultancy and other similar business services.
Kashish Vasan	User of allocated client’s information for assisting in performing business activities.

5. Vulnerability Statement

Vulnerability	Description
Common Data Server	All devices and users are connected to a central server. Thus, a user may become assessable to information for which he is unauthorized.
Common Mail	All information is received or sent through a common Mail address. So chances of assessabilty of unauthorized data and send unauthorized may occur.
BYOD Policy	Some users bring their personal systems for working in organization which may cause leakage of confidential data.
External hackers.	Though proper measure are taken to make IT security but there are always chances of external threats (Guided or Unguided)
System Failure	A software or hardware failure (accidental or otherwise) may cause loss of important data assets.

6. Threat Statement

Threat-Source	Threat Actions
Internal	Data Leakage, Unauthorized Access to E mail, Virus, IT System Crash
External	Theft, Hacking, Fire, Ransomware, Unauthorized Access, Password Cracking

7. Risk Assessment Results

Observation	Threat-Source/ Vulnerability	Existing controls	Likelihood	Impact	Risk Rating	Recommended controls
Data Leakage	Common Data Server	Server Password	Medium	Medium	High	Passwords, Logical access
Common E mail Acess	Common Mail Server	-	Low	Low	High	Separate user roles
Virus	Outside Factors	Antivirus	High	High	High	Antivirus software & Original Software, Access controls
Ransomware	Outside factors	-	Low	Medium	Low	Strong IT Security Policy
Data Confidentiality/ Access	BYOD	Server Password	High	High	Medium	Role based access policy
Outsider Access to Data	Password cracking	Server Password	Low	High	Medium	Strong Password Policy
System Crashing	IT/ Software & Hardware	Back ups	Low	High	High	Back up/ Cloud Storage
Pirated Softwares& applications	Softwares	-	Low	Low	Low	Original Software
Bring Your Own Device risk	BYOD	-	Medium	Low	Medium	-
Fire/ Short Circuit	Natural/ Accidental	MCB/ Fuse	Low	High	Low	AMC of Electric circuits
Theft	Outside Factors	Locks	Low	Medium	Medium	Insurance

Risk rating Matrix for the Risk Assessment

SCALE OF LIKELIHOOD		ACCEPTABLE	TOLERABLE	GENERALLY UNACCEPTABLE
	NOT LIKELY	Common E- mail Access	Pirated Software & applications	Loss due to fire
	POSSIBLE	Internal access to unallocated work	BYOD Risk	IT System Crashing
	PROBABLE	Outsider access	Data Leakage	Virus/Ransomware

IT Risk Mitigation & Security Policy

Risk Mitigation Policy &Procedures

Policy statement

Parshotam & Associates shall protect its information infrastructure and information generated/processed therein by building and maintaining robust information systems and processes.

The firm's employees/consultants, contractors, vendors and stake holders shall be committed to comply with all legal, regulatory, contractual policy and obligations by adhering to the practices defined to protect business sensitive and operational information.

Purpose

This policy states the intent of the firm to identify and protect its critical information assets. The principles of security adopted by the firm are:

- **Confidentiality:** Information shall be accessible only to those authorized.
- **Integrity:** Storage and processing methods shall ensure the accuracy and completeness of information.
- **Availability:** Information shall be available to those authorized when they need it.

The firm treats Information as the most valuable asset for its business. As the custodian of information that is either commercially, personally or business sensitive, the firm has a responsibility to protect that information from unauthorized or accidental modification, loss, releaseorimpactonthesafetyandwell-beingofindividuals.Furthermore,reliableinformation must be available to undertake the firm day-to-day business.

Specifically, information is crucial for supporting business processes and customer services, in contributing to operational and strategic business decisions, and in conforming to legal and statutory requirements. Accordingly, information must be protected to a levelcommensurate with their value to thefirm.

The purpose of information security management system is to protect the information of the firm, minimize business damage, and ensure business continuity by undertaking proactive measures for preventing and minimizing the impact of security incidents anddisasters.This Information Security policy defines the firm's expected code of conduct that is to be practiced, to ensure successful proliferation of Information Security culture at thefirm.

Policy sections andclauses

GENERALRESPONSIBILITY

It is the responsibility of all the firm employees/consultants, and contractors to comply with this and other associated policies. The ISTF (Information Security Task Force) Team is responsible for reviewing and, if required, revising this policy annually or as and when required.

Information Security Management System objectives

- To safeguard data and information to improve client and stakeholderconfidence.
- To provide a process framework for information securityimplementation
- To ensure compliance with Indian laws and regulations (for example IT Act 2008) as well as client contractual requirements for information security on an on-goingbasis.
- To ensure that all staff, relevant vendors and other personnel are covered under the information security awarenessprogram.
- To imbibe learning's from Incidents into the processes and establish a concrete Incident response mechanism to avoid furtherIncidents
- To improve information securityposture
- To ensure maximum availability of services to thebusiness.

Management Commitment Towards Information Security

Information, data and information systems in all its forms, including information about employees / consultants, clients and services, is among the most valuable assets of Parshotam & Associates. The security (confidentiality, integrity, availability, authentication, authorization and non-repudiation) of information is key to Parshotam & Associates culture and governance with regards to its clients and stakeholders.

The security of the information of each business unit is a responsibility shared by every employee/consultant within Parshotam & Associates Every employee/consultant and user within Parshotam & Associates or business partners and external entities have the obligation to ensure the confidentiality, integrity and availability of Parshotam & Associates electronic as well as non-electronic information and/or systems.

This Information Security Policy document has been established to provide management with direction and support, establish a security conscious culture and to provide the mandate to address Information Security risks throughout the firm. The management grants their full support and commitment to enforce Information Security, as outlined in this Information Security Policy document, on a firm level as well as within each of the business units.

Security Organization

An Information Security Committee shall be in place to ensure that there is a formal security strategy, clear direction and visible management support for security initiatives;

- The Information Security team shall maintain the ownership of the Information Security Policies and Procedures. It will be responsible for establishing, documenting, enforcing and distributing these policies and procedures and for keeping themup-to-date.
- Parshotam & Associates shall have a cross functional forum of management representatives from relevant parts of the organization to co-ordinate the implementation of information security controls;
- Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined;
- Advice on information security provided by in-house or specialist advisors shall be sought and communicated throughout the firm;
- Appropriate contacts with law enforcement authorities through the Legal Department, regulatory bodies, information service providers and telecommunications operators shall be maintained;

Risk Management Framework

To manage information security, the firm will adopt a process risk-based approach. Risk management will be performed on all the processes that are carried out by Parshotam & Associates. This will address unauthorized access, use, disclosure, disruption, modification and/or destruction of information or the information systemitself.

Risk management is the process of identification, assessment and treatment of risks. It shall identify known potential threats, the probabilityof their occurrence and the magnitude of the impact of those threats should they occur and ways to treating the risks.The risk management shall be reviewed and, where required, updated annually or whenever a significant change is made to the information system, whichever comes first.

This risk-based approach mandates:

- The identification of all critical services/processes/sub process.
- The identification of security vulnerabilities in the execution of these services/processes/sub-processes
- The identification of threats and threat probabilities that may result in exploitation of the vulnerabilities.
- The identification of the proper set of controls to protect these services/processes from the identified threats. Controls should also be identified in line with any required guidelines or contractual clauses on information security.
- The proper business continuity solutions to deal with loss of key assets processes, people, or physical premises.
- The assessment of risk at least annually to ensure it is being adequately managed, and previously identified risks are being addressed.
- Maintain information security in line with laws, regulations, contractual obligations and management best practices as adopted by the firm.

SECURITY AWARENESS PROGRAM

An information security management system will continue to grow and maintain itself only if the people of the firm are continuously vigilant and are able to absorb information security principles in their work culture.

- In accordance with this statement, it is essential for firm to implement security awareness initiatives at all levels of the firm, including senior management, middle management, head of the departments, support staff and any third parties.
- The information security awareness sessions will be an ongoing initiative which will ensure that all the employee / consultants and contractors are aware of the information security policies that are relevant tothem.
- In addition, this shall include all the procedures, guidelines, and information security best practices in conjunction with other laws, regulations, and management best practices as adopted by the firm.

Security Policies Requirements

Password Policy

- All computing accounts shall be protected by strong passwords. Account holders and system administrators shall protect the security of those passwords by managing passwords in a responsible fashion.
- All system-level passwords (e.g., root, enable, Windows admin, application administration account etc.) must be changed on regular basis.
- All user-level passwords must be changed at least every 90 days
- Default passwords for hardware and software must be changed prior to implementation
- All user-level and system-level passwords must conform to the guidelines described below
- Poor, weak passwords have the following characteristics:
  1. The password contains less than eightcharacters
  2. The password is a word found in a dictionary (English or foreign) X The password is a common usage word suchas:
  3. Names of family, pets, friends, co-workers, fantasy characters,etc.
  4. Computer terms and names, commands, sites, companies, hardware, software
  5. The words "<company Name>", or anyderivation
  6. Birthday's and other personal information such as address and phone numbers
  7. Word or number patterns like aaabbb, qwerty, ztxwvuts, 123321, etc. X Any of the above spelledbackwards
  8. Any of the above preceded or followed by a digit(e.g., secret1,1secret)
- Strong passwords have the following characteristics:
- Contain both upper- and lower-case characters (e.g., a-z,A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9,@#$%^&*()-_=+|\}]{["':;?/>.<,~`
- Are at least eight alphanumeric characterslong
- Are not words in any language, slang, dialect, jargon,etc.
- Are not based on personal information, names of family,etc.

Password should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation or other phrase. For example, the phrase might be:" This May Be One Way To Remember "and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some othervariation. Password Policy ensures that a user password is strong and is changed in a periodic manner so that it becomes highly impossible for an attacker to crack the passwordfollowing in Domain controller:

- Maximum Password Age :- 120days
- Minimum Password Length :-8
- Passwords must meet complexity requirements

INTERNET

Internet should be used only for business purposes. Internet access should be controlled to ensure that only business-related sites are accessible.

NETWORK

- User access to the network should be authenticated
- When the user leaves the organization all the network access shall be removed as per Logical access control policy and procedure
- Network access should be granted only after necessary approvals.
- Administrative access to the network and security devices should be controlled.
- Physical access to the network and security devices should be controlled.
- Where ever possible all confidential data that is sent over the network should be in encrypted format.
- Clock time should be synchronized.

PATCHUPDATING

Servers, desktops/laptops and applications shall be frequently patched to protect against widespread worms and malicious code that target known vulnerabilities on unpatched systems.

NON-ESSENTIAL SERVICES

- All application and OS services that are not essential for the functioning of the system should be disabled.
- Disable default accounts or change password
- All the unused hardware ports of the system should be disabled from the OS to prevent any malicious activity using those ports.
- Disable unwanted ports like CD/DVD, USB, Serial port.

LOGINBANNER

Operating system should have an initial login message configured stating that the system should be used only for authorized activities

ANTI-MALWARE

Window Defenders is being used to minimize malware.

Display

- Machine inactivity limit security policy, the device locks not only when inactive time exceeds the inactivity limit, but also when the screensaver activates or when the display turns off because of power settings.

- Set Inactivity limit as 15 minutes.

PHYSICAL

- A clear desk and screen policy, all employees to lock their computers when leaving their desk and to log off when leaving for an extended period oftime.
- Employee shall keep printed documents under locked when not inuse
- Employee shall not leave printout near printer desk and conference room.

Security Metrics AndMeasurement

In addition to maintaining the information security management system, it is imperative to monitor and measure the ongoing efforts and results of the information security management system. Therefore, effectiveness metrics shall be identified for specific controls implemented in the firm. The procedure will also identify techniques for implementing and reviewing measurements of the identified metrics. The inputs and outputs to the measurements will be reviewed on a regular basis in line with the procedure. In addition to the specific controls, the stated ISMS objectives would be measured to ensure that they meetexpectations.

Legal Or Regulatory Requirements

The primary laws and regulations with which the firm needs to comply are defined as a part of the ISMS (Information Security Management System) Scope document.

Policy AndImplementationReview

Reviews of the Information Security policies and their implementation shall be carried out regularly by an independent body (e.g.: internal audit function, an independent manager or a third-party organization). This review will happen under the followingcircumstances:

- At least once in a year.
- If there is a significant change in the technologies in use.
- If there is a significant change in the external threat environment, which mandates a review of the risk profile.
- If there is a significant change in requirements/guidelines for information security.

Enforcement

Necessary disciplinary action will be taken against any employee / consultant not following the policies and procedures laid down by Parshotam & Associates. Similarly, action will be taken against those employees / consultants encouraging/ observing such an activity and not reporting the same to the concerned authority. Any employee / consultant found to have violated or not practicing his/ her role may be subject to disciplinary action, up to and including termination of employment as per Parshotam & Associates HRpolicies.

Definitions /Acronyms

Definitions

Term	Explanation
Firm	Parshotam & Associates
Asset	Anything that has value to the firm.
Information Security	Preservation of Confidentiality, Integrity and Availability; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved
Information Security Management System	The system designed, implemented and maintained for assuring coherent suite of processes and systems; for effectively managing information accessibility, thus ensuring the confidentiality, integrity and availability of information assets and minimizing information security Risks
Scope	Extent or range of view, outlook, application, operation and effectiveness for planning, implementing, checking and acting upon w.r.t. Information Security Management Systems
Employee	Person hired to perform a job or service for the firm, and one who is directly employed or hired on a contract basis
Consultant	Law Professionals
Vendors	Allthirdpartieswhichincludes,butisnotlimitedtovendors,volunteers, contractors, consultants, temporaries, and others who have access to, support, administer, manage, or maintain the firm's information or physical assets
Shall	Mandatory Action
Should	Preferable Course of Action

Acronyms

Acronym	Full Name
ISMS	Information Security Management System
IT	Information Technology
ISTF	Information Security Forum
ISO	International Organization for Standardization