Effective from 1st February, 2016

TABLE OF CONTENTS

1. Introduction

Parkar Consulting Group ("PCG" or the "Company"), Information Security Policy (the "the policy") is designed to provide instruction for the protection of all information assets commensurate with their sensitivity and criticality to PCG, their potential for misuse, regulatory requirements, and current industry practice.

The Company uses information assets to deliver the services and protection of all information assets and any technology resource supporting the business processes is critical for business viability. Information assets are faced by several potential risks caused due to errors, malicious and/or criminal activity, systems failures or natural disasters. Such risks may result in loss of or damage to information assets. Additionally, in its course of business PCG receives, uses, creates, stores, maintains and/or transmit information of its own, its client's and/or its customer's. Due to the confidential nature of such information as well as the criticality of the information assets in use, it is imperative that the Company safeguards the information based on three basic principles of Information Security: Confidentiality, Integrity and Availability.

Confidentiality – It is directly related to the criticality, sensitivity and value of any information. The information must only be accessible by those individuals, processes and systems (collectively known as "entities") that have a business need-to-know and are authorized to access it. It must not be disclosed or made available to unauthorized entities.

Integrity – It is directly related to the required accuracy and completeness of any information. The information must not be modified without authorization as well as the means through which the information is accessed must also be validated.

Availability – It is directly related to ability to access any information asset when needed or required by authorized entities.

2. Purpose

The purpose of this policy is to outline security related policies at a high level. The statements in this document provide minimum security standards and apply to all personnel, systems, networks and business areas. These standards are required to ensure compliance with legal, regulatory, contractual and business requirements as well as they reflect the Company's commitment to safeguard the security, confidentiality, and integrity of its information and information technology assets.

3. Scope

The policy is applicable to any data created, collected, processed, stored, maintained or transmitted using any computer systems, data storage systems, networks, applications, communication systems, and mobile devices. It also applies to all personnel including, full and part-time employees, contractual employees, clients, customers, business partners/vendors, suppliers, service providers (Non-Disclosure Agreement must be in place prior to access provisioning for all personnel), and any other third party that has access to PCG IT resources.
The policy applies regardless of the means (remotely or directly) or systems used to conduct Company business and/or access information of the Company, its clients and/or customers.
For the purpose of this document, personnel are described throughout this policy as following:

- Associate refers to PCG full-time employees.
- Non-Associate refers to part-time employees, contractors, customers, clients, business partners/vendors, suppliers, service providers and others.
- Users refer to both Associates and Non-Associates.

4. Distribution

This is an Internal-Use Only document belonging to PCG. Distribution must be limited to Company associates and non-associates who are subject to a NDA. Any other use or distribution of this policy must be approved by the PCG Management.

5. Compliance

5.1. PCG must identify compliance requirements based on legal, regulatory as well as contractual requirements. Compliance requirements must be documented and reviewed periodically.

5.2. All users are required to comply with this policy and failure to comply will result in disciplinary action up to and including termination.

5.3. All users must acknowledge their understanding and acceptance of Information Security Policies, processes, and procedures on an annual basis.

5.4. PCG Information Security Team and/or Internal/External Audit team must assess and report on compliance to this policy on an annual basis, at the least.

6. Roles and Responsibilities

6.1. PCG Management

- Responsible for protection of Company's Information Assets and maintaining a safe and productive work environment.
- Responsible for review and approval of Information Security Policy and associated policies on an annual basis.
- Responsible for approving any substantive modifications, supplements, or amendments to the Information Security Policy.
- Provide support for implementation and enforcement of Information Security Policy.

- Provide adequate resources (Human and Capital) for appropriate implementation of Information Security policy.
- Promotion of Information Security across the company through clear direction about and a demonstrated commitment to information security.

6.2. Information Security Team

- Custodian of Information Security Policy and all related policies, processes, procedures, standards and baselines.
- Monitor Information Security Requirements based on client, customer, business, regulatory, legal and contractual requirements and changes to the same.
- Recommend changes to Information Security Policy and all related policies, processes, procedures, standards and baselines to Management.
- Conduct on-going risk assessment and identification of controls for risk mitigation.
- Responsible for implementation and enforcement of Information Security Policy.
- Conduct Awareness sessions for Information Security.
- Report all Information Security Violations to Management and Human Resource Team.
- Identify and record Information Security Requirements in all contracts signed by PCG with clients and/or third parties.
- Implement Information Security Requirements identified as per contractual obligations.

6.3. Users

- Comply with Information Security Policy and all related policies, processes, procedures, standards and baselines as well as any additional implemented controls as per customer or client requirements.
- Report any deviations from policy to Information Security Team.
- Report any and all security incidents, suspected or otherwise, to Information Security Team.
- Protect Company, customer and/or client confidential information.

6.4. Others

- PCG's Human Resource Team is responsible for addressing disciplinary actions for reported violations for Associates.
- PCG's Human Resource Team is responsible for forwarding all reported violations for Non-Associates to concerned HR Departments.

7. Segregation of Duties

7.1. The integrity and security of Company's business activities, its data and information systems must be ensured by applying Segregation of Duties.

7.2. Segregation of Duties must be established and documented in order to ensure that an individual does not have access to more than one critical task as defined by the management.

7.3. It should be used as an assistance tool to ensure mitigation of risks against malicious or inadvertent breach of system security, data integrity, or the disruption of normal business operations.

For examples of Segregation of Duties, please refer to Appendix A.

8. Third Party Management

8.1. All engagements with third parties (vendors) for IT Infrastructure and services must be addressed with appropriate due diligence.

8.2. Any contract or procurement document created and/or executed between PCG and any third-party (vendor) entailing service provisions for creation, processing, handling, storing, maintaining and/or accessing information of company, its clients and/or customers must address security requirements outlined in Security Exhibit Document.

Note: The Security Exhibit Document must be attached to the contract or procurement document where applicable. Please refer Appendix B for Security Exhibit Template.

8.3. All appropriate and applicable policies, processes, and procedures must be followed by third-party (vendors) and the same will be shared on need-to-know basis by PCG.

8.4. It is the responsibility of the Vendor Management Team to ensure adherence to requirements outlined in Security Exhibit by the vendor.

8.5. In an event a third party requires access to PCG's network and/or systems, a security risk assessment must be conducted to document risks associated with the activity. PCG Management must review the identified risks and take appropriate actions for risk mitigation.

8.6. Access to PCG network and systems will be granted post review and approval by management on risk mitigation action plan.

9. Information Security Risk Management

9.1. A periodic information security risk assessment must be conducted against all identified assets in order to identify and evaluate risks faced by the Company. *Please refer Risk Assessment Process and Procedure for information on how to conduct a Risk Assessment.*

9.2. Guidance and recommendations must be provided to management for all identified risks.

9.3. Security Risk assessment report must provide the following:

- Name(s) of the asset(s) against which the assessment is carried out.
- Identified Security threats and vulnerabilities for the asset.

- Estimation of the likelihood of the risk materializing.
- Calculated Risk Rating.
- Identified existing controls that can be implemented to reduce the impact to business or the likelihood of the risk materializing.
- Expected new risk rating based on the implementation of existing controls.
- Documented residual risk (if any).
- Requirements for risk mitigation (legal, financial, contractual or regulatory requirement) in detail.
- Recommendations for risk mitigation, to an acceptable level, including implementation of existing or new controls and risk mitigation strategy.

9.4. All identified information security risks must be evaluated and documented in Information Security Risk Register. (*Please refer Asset and Risk Register Workbook)*

9.5. Risk Management of identified risks will be carried out as Risk Mitigation strategy outlined below.

9.5.1. Risk Transfer Strategy – the risk is transferred to a third party, e.g., purchase of insurance, subcontracting the activity, etc.

9.5.2. Risk Acceptance Strategy – the risk is accepted by Management due to business reasons, e.g., the cost of risk mitigation is higher than the impact to business if the risk materializes, or if the likelihood and impact of the risk acceptable.

To ensure that IT risk management decisions are tied to accountability for identified risks, a risk acceptance memo will be generated by an Associate. The approval will be granted through appropriate signoff as determined by the PCG Management.
All approved risk acceptance are valid no longer than one (1) year and must be reviewed and recertified if there is a need for extension. Please refer Appendix C for Risk Acceptance Form Template.

9.5.3. Risk Avoidance Strategy – the activity involving the information asset resulting in the risk is eliminated.

9.5.4. Risk Reduction Strategy – Controls that are identified as part of recommendations for risk management must be selected and/or implemented to reduce risk to an acceptable level and must meet business requirements. The acceptable level is determined by Management while considering the following:

- Any legal, regulatory or contractual obligation.
- Business objectives
- Operational requirements.

10. Physical and Environmental Security

10.1. All physical areas used to conduct business activities must be classified based on the sensitivity, criticality and value of the information assets located in the specified area. The identified areas of business are classified as below:

Area Classification	Description	Examples
General	No Information Assets are present in this area.	Reception Area, cafeteria, etc.
Level 1	Limited Information Assets are present.	Meeting rooms, waiting rooms, etc.
Level 2	End-user Information Assets are present	General Work Areas
Level 3	Critical Information Assets are present	Server Room(s), Compactor Room (s), Executive Offices, etc.

10.1.1. Additional requirements for physical security may be present due to legal, regulatory or contractual obligations and PCG must ensure compliance with such requirements.

10.2. Appropriate controls and measures must be enacted and implemented based on physical area classifications, such as access cards, locks, etc.

10.3. PCG datacenters must have a physical security plan which are reviewed annually but may require updates on regular intervals based on business requirements.

10.4. Physical access management process and procedures must be created to ensure appropriate guidelines are followed for access provisioning and revocation.

10.5. Access for visitors and third-parties to PCG facilities must be monitored at all times and reviewed regularly.

10.5.1. Visitors will not be provided access to Level 3 classified areas. If access is required, the visitor must be escorted at all times to any such areas.

10.5.2. Visitors must be escorted at all times in Level 2 classified areas.

10.5.3. Visitors are prohibited from bringing personal items into Level 2 and 3 classified areas, which could be used to obtain, transmit, hold or store data of PCG, its clients and/or customers, without prior approval.

10.6. A risk based approach must be followed to identify appropriate controls for protection against external and environmental threats, such as damage form fire, flood, earthquake, explosion, civil unrest and other forms of man-made or natural disasters.

10.7. Access to areas to be used for delivery and loading/unloading must be controlled and where applicable segregated from any areas classified as Level 1 through Level 3.

10.8. All critical information assets must be protected against power failures or other disruptions from utilizes.

10.9. Access to cabling and infrastructure providing communication services must be implemented to avoid risks such as damage, unauthorized interception, etc.

10.10. A risk based approach must be followed for allowing off-site movement of any information asset containing data belonging to the Company, its clients and/or customers.

10.10.1. Management approval is required for any off-site movement.

10.10.2. Data owners and users are responsible for ensuring compliance with all policies, processes and procedures when off-site.

10.11. Any information asset containing non-public information must be appropriately destroyed (rendered inaccessible and/or readable) prior to disposal.

10.12. Any redeployment of an electronic media or computer equipment must be carried out post complete asset sanitization.

10.13. Any information asset subject to any investigation (legal, compliance, criminal, etc.) must not be sanitized, destroyed and/or disposed of.

10.14. Any loss of an information asset must be reported immediately to IT Support Team.

11. Human Resource Policy

11.1. Prior to Employment

11.1.1. Information Security roles and responsibilities must be identified for each defined role in the organization and must be communicated to prospective employees as part of recruitment process. The roles and responsibilities may be incorporated in adequate job descriptions and/or in employment terms and conditions.

11.1.2. Background verification must be completed for all prospective employees, including but not limited to, full-time employees, contractors, third-party vendors, etc.

Note: For Non-Associates background verification should be done by business partners/vendors providing the resource and proof of the same must be provided to PCG and validated by PCG.

11.1.3. Any employee contract (such as Offer letter) must outline the security requirements of both the employees and the Company. The employee must agree to any such terms and conditions of employment prior to being provided access to PCG information assets.

11.2. During Employment

11.2.1. All employees, including contractual employees, must comply with all policies, processes and procedures.

11.2.2. PCG Management and an employee's manager are responsible for ensuring that all employees are aware of Information Security policies, processes and procedures as well as their roles and responsibilities.

11.2.3. PCG Management must ensure an on-going awareness and training program is in place for all employees. The program must contain current and relevant information regarding Information Security and any changes to the security posture of the organization including new policies, processes or procedures.

All employees are required to participate in an awareness refresher training on an annual basis.

11.2.4. Disciplinary action will be initiated against any employee found to have committed an Information Security policy violation. The disciplinary action will vary and includes actions up to and including termination.

Information Security Team is responsible for informing Management as well as Human Resource Department of any and all violations by users.

11.3. Termination or Change of Employment

11.3.1. Human Resource Department is responsible for initiating termination of employment or employee exit process. HR Team must inform Information Security and IT Support Team prior to an exit or termination in order to ensure appropriate controls can be implemented for data preservation, such as data backups, access revocation, etc.

11.3.2. An employee's manager is responsible for ensuring that any and all assets of the Company are returned prior to an employee's exit from the organization. These assets include, but are not limited to, laptops, mobile devices, documents, storage cabinet keys, electronic storage media and physical access cards among others.

11.3.3. In an event of where the role of an employee is subject to change, it is the responsibility of current and new manager to ensure that employee's access to systems, information, databases, applications, etc. is appropriately modified based on need-to-know and need-to-have principle.

11.3.4. In an event of urgent separation, the system(s) of the employee must be segregated from the Company's network and logical access (Enterprise IDs, system accounts, etc.) removed to prevent back doors, Trojan horses, viruses, or any other unauthorized software from being introduced to Company's network or system.

It is the responsibility of HR Team to inform Information Security Team and IT Support Team of any urgent separations.

12. Client Management

12.1. In the course of business PCG may provide various IT services from their premises to its clients. As such, PCG must ensure that a Statement of Work (SOW) is executed between the concerned parties to outline the nature of the service to be provided and the mode in which it will be provided.

12.2. PCG must ensure that a Memorandum of Understanding (MOU) is signed with any client to whom services are rendered utilizing PCG assets and infrastructure to outline roles and responsibilities of each party.

12.3. PCG must ensure that all Legal and Compliance requirement of the client are captured and addressed either through a SOW or a MOU.

13. Information Asset

13.1. PCG Information assets include, but are not limited to, physical and virtual systems, network appliances and systems, and data of PCG and its employees, customers and/or clients.

13.2. An inventory of all critical assets must be created and maintained.

13.3. Appropriate access controls must be maintained and supported for all information assets.

13.4. "Owners" of Information assets must be identified by Data Stewards for all identified information assets. The owner must classify each asset as per Information Classification Policy and identify, implement, enforce and maintain appropriate controls for each asset based on its classification.

14. Information Classification

14.1. All information assets must be classified in order to determine necessary security controls required to protect such assets.

14.2. Information assets are classified as one of the following categories based on the value, sensitivity, criticality, legal and regulatory requirements and contractual obligations:

14.2.1. **Confidential**: any information asset that is extremely critical to PCG and its disclosure could lead to compromise of the privacy of users, customers and/or clients, reduce the Company's competitive advantage or adversely impact the Company or its business. Such information assets include, but are not limited to, sensitive corporate, legal, financial, human resource or personal information.

Note: All information belonging to/regarding clients or customers is classified as confidential unless otherwise communicated in writing.

14.2.2. **Intellectual Property (Proprietary)**: any information asset that has a significant business value and any unauthorized disclosure or dissemination would lead to severe damage to the Company. Such information assets include, but are not limited to, business strategy model, pricing strategy, marketing strategy, source code, application logic, brands, logos, etc.

14.2.3. **Internal-Use Only:** any information asset of a specific value to the organization, and unauthorized disclosure or dissemination of which could impact profitability or market share of PCG. Such information is usually confidential and/or proprietary but management or data owners have approved wider audience for the same within the organization. Examples of such information assets include, but are not limited to, business update communication, internal re-organization, policies, processes, procedures, etc.

14.2.4. **Public Information:** any information asset that has been made available for public consumption through Company approved communication channels. Such information assets include, but are not limited to, press briefings, published annual reports, offered services, etc.

15. Information Protection

15.1. Controls must be established for protecting information assets based on their classifications.

15.2. Identified controls must be reviewed and approved by Information Security team and management prior to implementation.

15.3. The Company must ensure that safeguards are in place against unauthorized copying and/or redundant authorized copies of sensitive/confidential information.

15.4. Access to information assets must be granted based on need-to-know and need-to-have principles.

15.5. Personal data of employees, users, clients and customers, collected by PCG as part of business operations must be protected.

16. Logical Access Control

16.1. Management, monitoring and control of access to PCG Information Assets will be based on sensitivity, criticality, and value of such assets and in accordance with need-to-know and need-to-have business and legal requirements.

16.2. Managers are responsible for ensuring notifications to business and applications teams, Human Resources, IT and Information Security Teams regarding a user's exit or role change.

16.2.1. Business and application teams are responsible for granting and managing access based on business requirements.

16.3. Access management procedures must be followed for granting, reviewing, and revoking access to information assets.

16.4. The concept of 'least privilege' must be followed for access to information assets.

16.5. Access controls must be implemented for all users, including third-party, for access to information assets.

16.6. Elevated privileges must be reviewed on quarterly basis for all information assets.

16.7. Password Management Standard must be followed for access controls.

16.8. All users are required to follow best security practices to ensure protection of information assets.

16.9. Access to network services will be based on business requirements and must be controlled on need-to-have basis.

16.10. Remote access will be granted only through secure means such as SSL or IPSec VPN.

16.11. PCG internal network (Wired and Wireless) must be segregated for each client and/or customer and access controlled for appropriate users.

16.12. Access to network shares and/or printing services must be controlled based on business requirements.

16.13. All PCG systems, network, and other information assets must have access control configured based on a user's Unique Identifier ("User ID").

16.14. User IDs must be provisioned for each user and sharing of the ID and password is strictly forbidden.

16.15. Users will be required to authenticate using one of the following methods:

- Passwords
- Passphrases
- Multi-factor authentication (e.g., smart cards, biometrics and tokens among others).

16.16. PCG support teams have the right to restrict access to information assets.

16.17. Physical and Logical segregation must be maintained between “sensitive” information assets and other assets.

16.18. Use of personal devices for PCG purposes is strictly forbidden and company owned devices must be configured, managed, and maintained as per established policies, processes and procedures.

17. Anti-virus

17.1. All systems used for business activities must have centrally configured and managed security software for protection against viruses, malware and spyware.

17.2. The anti-virus software must have updated virus definition files on all systems and must scan for infections in real time as well as weekly scheduled scans.

17.3. Any system identified as being infected must be segregated from Company network immediately and the infection or infected files must be cleaned, quarantined and/or deleted before being allowed back on network.

18. Application Security

18.1. All applications must be configured to allow user authentication against Company's Directory Services only.

18.2. All applications that create, modify, maintain, handle, and/or store data belonging to PCG, its clients or customers, must be developed using secure development methodologies (e.g., SANS, OWASP, etc.)

18.3. All architectural designs, work flow diagrams, and data flow diagrams must be reviewed for potential security risks.

18.3.1. All identified risks must follow Risk Mitigation Process.

18.4. Applications must follow Change Management Policy, processes and procedures for deployment, updates and support.

18.5. Any application undergoing development, testing or QA must not use production data for the same.

18.6. Application infrastructure must be physically and/or logically segregated from databases containing information required by the application.

18.7. All applications must go through security assessment and review prior to being moved to production.

18.8. Encryption must be used by applications for authentication, data transmissions and storage.

18.9. Applications logs must be monitored and maintained for:

- Errors encountered by application.
- Access and/or authorization provisioning.
- Actions carried out by elevated privileges.

19. Databases

19.1. Databases containing confidential information must use encryption for data-at-rest and data-in-motion.

19.2. Access to databases and data contained within must be restricted to database administrators and application accounts.

19.3. Databases containing data of multiple clients and/or containers must be physically and/or logically segregated.

19.4. Databases logs must be maintained for:

- Errors encountered by Database.
- Access provisioning for users and applications.
- Actions carried out with elevated privileges.

20. Encryption

20.1. All user systems must be encrypted with encryption software that is centrally managed.

20.2. All electronic information classified as confidential must be encrypted regardless of storage location.

20.3. Key sizes to be used at minimum are: 256 bit key size for symmetric encryption and 2048 bit key size for asymmetric encryption.

20.4. All keys used for encryptions must be renewed on an annual basis.

21. Mobile Devices

For the purpose of this policy and any related documents, mobile devices are identified as cell phones, tablets, and other smart devices.

21.1. Only company-owned or approved mobile devices are to be used to carry out business related activities.

21.2. Use of personal or non-PCG devices must be approved by PCG Management and Information Security Team.

21.3. All personal devices approved to be used for business activities is subject to complete wipe upon user separation.

21.4. All non-PCG devices used for business activities must be in compliance with all PCG policies.

21.5. Any unauthorized or unapproved device connected to Company network is subject to disconnection and confiscation as well as being forbidden from Company network for all future requirements.

22. Data Backup

22.1. Backups will not be provided for end-user systems (laptops, desktops, mobile devices, etc.). Users must store all business related data on approved data storage locations only.

22.2. Backups of critical infrastructure, system configuration and network configuration must be maintained in the following manner:

- Full backups to be conducted once a week.
- Incremental backups to be conducted daily.

- Configuration files backups to be conducted post any change implementation.

22.3. All backups must be tested regularly to ensure data validity, verification and accessibility.

23. Removable Media

23.1. Use of removable media (USB keys, external hard drives, optical devices, etc.) to store company data and information is strictly forbidden.

23.2. Written approval from Information Security team, based on valid business justification, is required prior to use of removable media for any work related activity.

23.3. Any removable media used for business activities must be sanitized prior to being redeployed, reused or disposal.

24. Protection Against Mobile and Malicious Code

24.1. A risk based approach must be followed for identification of required controls to protect against malicious and mobile code. The controls must provision for prevention of, detection of, and recovery from such code.

24.2. The controls must address the requirements of blocking, restricting or isolating such code.

25. Vulnerability Management

25.1. All assets used to carry out PCG business activities must be subjected to vulnerability assessment regularly to identify risks to the company, data and infrastructure.

25.2. All identified vulnerabilities must be addressed as per Risk Management policy, processes and procedures.

25.3. Identified vulnerabilities must be classified as below and addressed accordingly:

- High Vulnerabilities: A vulnerability that may result in catastrophic and significant physical or property damage or loss, loss of revenue or productivity (e.g., Denial of Service Attack, buffer overflows, or source code exposure, etc.) upon exploit. Any such vulnerability must be addressed within eight (8) hours from discovery.

- Medium Vulnerabilities: A vulnerability that may result in moderate physical or property damage or loss, loss of revenue or productivity (e.g., weak encryption, possible phishing opportunity, etc.) upon exploit. Any such vulnerability must be addressed within 48 hours of discovery.

- Low Vulnerabilities. A vulnerability that may result in minor physical or property damage or loss, loss of revenue or productivity (e.g., missing patch, use of FTP, etc.). Any such vulnerability must be addressed within seven (7) working days of discovery.

26. Wireless

26.1. Wireless network must be available to carry out business activities and must be segregated for each client and/or customer.

26.2. Data transmissions between end users systems and wireless infrastructure must be encrypted.

26.3. Authentication to wireless network must be based on User IDs.

26.4. Regular inspection must be carried out for rouge wireless access points and devices.

27. Information Security Incident Response

27.1. Effective and efficient Incident Response process and procedures must be maintained to identify possible security incidents, their impact on business and response towards the incidents in a timely manner.

27.2. The process and procedure must enable quantification of business impact due to a security incident based on type of incident, volume of impacted assets and cost of recovery or damages.

27.3. Incident Reporting

27.3.1. All users must inform Information Security Team of any suspected security incident.

27.3.2. Information Security Team must review logs of all security tools on a daily basis to identify any suspected security incidents.

27.3.3. Information Security must inform business, application and other support teams impacted due to a security incident.

27.3.4. Management must communicate to clients and/or customers regarding possible security incidents involving their information assets.

27.4. Incident Management

27.4.1. All incidents will be addressed by Information Security team in conjunction with other relevant business, applications and/or support teams.

27.4.2. All incidents must be recorded in an Incident tracker with relevant information. The information must be reviewed regularly to identify additional safeguards and controls that need to be implemented in order to prevent reoccurrence of similar incidents.

27.4.3. Any security incident resulting in a legal action (civil or criminal) against an entity or an individual must adhere to evidence collection and preservation requirements as per applicable law, rules and regulations.

28. Business Continuity Management

28.1. Business Continuity and Disaster Recovery related processes and plans must be created, tested, and maintained to ensure continued business operations in an event of a disaster.

28.2. Management designate an individual that must serve as Business Continuity and Disaster Recovery Program Manager, whose responsibilities will be:

- Identification of assets to be governed by DR and BC Plans.
- Creation and maintenance of DR and BC Plans.
- Regular testing of established plans (scheduled and unscheduled).
- Identification of threats that may have an impact on business; the likelihood of the threat materializing and the risk to business based on likelihood and impact.

29. Capacity Planning

29.1. IT Support Team will be responsible for carrying out capacity planning for IT Infrastructure, software and application licensing as well as inventory management.

29.2. Based on capacity plans, IT Support Team must address business needs in a timely manner, e.g. procuring additional application licenses based on recruitment projections.

30. Acceptable Use Policy

Please refer Acceptable Use Policy document available here.

31. Policy review

Information Security policy must be reviewed at the least on an annual basis or if the compliance requirements for PCG have significant changes as per Policy Review Process and Procedure.

32. Exceptions

32.1. A policy exception request must be raised in writing, by an associate, to Information Security Team and the request must be reviewed and approved by Information Security Team and PCG Management before the exception is valid.

32.2. All exceptions will be valid for no longer than a year (1 year) and all approved policy exceptions must be stored for a period of three (3) years.

Evidence of approved exceptions must be documented, stored and available upon request.

Appendix A – Segregation of Duties

Sample segregation of duties includes, but is not limited to, the following:

- Software Developers should not have access to production systems, unless specifically authorized by the data/system owner.
- Access to network security systems should be limited to the Information/Network Security teams.
- Access to system logs and system audits should be limited to Information Security or Internal Audit Team.
- Database Administrators should only have access to Databases and must not have root or administrator access on the Database Server.

Appendix B – Information Security Exhibit

Security Exhibit.docx

Appendix C – Risk Acceptance Form

Risk Acceptance Form.docx

Glossary

Access Control	It means to ensure that access to assets is authorized and restricted based on business and security requirements.
Access Provisioning	The process of providing users with appropriate credentials to access information assets.
Access Revocation	The process of revoking user credentials used to access information assets.
Asset Sanitization	The process of removing information completely from a system or storage device so that the information cannot be retrieved, even from forensic capability. NIST (special publication 800-88) provides proper destruction methods for media sanitization.
Authentication	Provision of assurance that a claimed characteristic of an entity is correct, i.e. verification of who an entity is.
Authorization	Process of verification that an authenticated entity is authorized to access an information asset.
Availability	Ability to access any information asset when needed or required by authorized entities.
Business Continuity	It is the planning, preparation and other related activities involved in ensuring that an organization's critical business functions and assets continue to operate or will be recovered in an operational state within a reasonable short period of time in an event of a disaster or incident that may impact the organization.
Communication Systems	Systems used to ensure communication capabilities between entities, such as networking equipment, Wireless access points, digital and analog phones, etc.
Computer Systems	A programmable machine designed to sequentially and automatically carry out a sequence of arithmetic or logical operations.
Confidential	Any information asset that is extremely critical to an organization and its disclosure could lead to compromise of the privacy of users, customers and/or clients, reduce the Company's competitive advantage or adversely impact the Company or its business
Confidentiality	It is directly related to the criticality, sensitivity and value of any information. The information must only be accessible by those individuals, processes and systems that have a business need-to-know and are authorized to access it.
Data Owner	An entity that can authorize or deny access to certain data and is responsible for accuracy, integrity and timeliness of the same.
Data Steward	An entity that is responsible for planning, implementing, and managing the sourcing, use and maintenance of data assets in an organization.
Database	A collection of (usually) organized information in a regular structure, usually but necessarily in a machine readable format accessible by a computer.
Datacenter	It is a facility used to house computer systems, and associated components like telecommunication systems, networking components and storage systems.
Disaster	A disaster is a natural or man-made (or technological) hazard resulting in substantial physical damage or destruction, loss of life, etc.
Disaster Recovery	It is a process, policies, and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a disaster.
Disclosure	It is an action that makes confidential information known with or without authorization.
Elevated Privileges	Elevated privileges allow a user to perform certain activities on a system that general users do not have authorization to conduct.

Entities	Individuals, processes and systems are collectively known as entities.
Information Assets	It is any data, device, or other component of the environment that supports information related activities.
Integrity	The accuracy and completeness of the information is called integrity.
Intellectual Property	Any information asset that has a significant business value and any unauthorized disclosure or dissemination would lead to severe damage to the Company.
Internal-Use	Any information asset of a specific value to the organization, and unauthorized disclosure or dissemination of which could impact profitability or market share of PCG.
Least Privilege	A principle that requires every user or process to only have those privileges that are absolutely necessary to carry out their roles and responsibilities.
Mobile Devices	Includes tables, cell phones and other devices that can function from remote locations with network connectivity.
Need-to-have	It is a principle that identifies the access required by a user or process on information assets to carry out their roles and responsibilities.
Need-to-know	The necessity for access to, knowledge or possession of, specific information required to carry out official duties.
Network	A group of two or more computer systems linked together.
Public	Any information that has been identified for public consumption through authorized communication channels.
Removable Media	Any time of storage media that can be removed from a computer system while the system is still operational.
Risk	It is the effect of uncertainty on objectives.

Risk Acceptance	It is a conscious acceptance of the fact that a risk exists for a particular information asset, project, etc. Usually this acceptance occurs when the cost of risk mitigation is higher than the impact faced by an organization if the risk materializes.
Risk Assessment	A systematic process of evaluating the potential risks that may be involved in a project activity or undertaking or to an information asset.
Risk Avoidance	It is the process of not carrying out any activities that can carry a risk.
Risk Mitigation	The actions taken to mitigate identified risks.
Risk Reduction	The actions that can reduce the impact to an organization if an identified risk materializes.
Risk Transfer	The action to transfer the monetary impact to an organization due to a risk such as an insurance policy.
Security Incident	The attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.
Sensitive Information Assets	Any asset that requires protection due to risk and magnitude of loss or harm that could results from its inadvertent or deliberate disclosure, alteration, or destruction.
Software/Application	The programs or other operating information used by a computer/end-user.
Source Code	A text listing of commands to be compiled or assembled into an executable computer program.
Vulnerability	It is the weakness of an asset or control that can be exploited.

Version Control

Date	Prepared by	Reviewed by	Action
10 March, 2016	Aniket Jadhav	Gaurav Singh	Created Policy