Client Data Protection Policy

Policy Reviewed / Revised: December 2024

Related Items:

- PCG Employee Handbook

Purpose

Project Consulting Group ("PCG") has adopted the following Client Data Protection Policy ("Policy") as a measure to protect the confidentiality, integrity, and availability of Client Data.

Scope

This Policy applies to all Employees and Sub-Contractors of PCG.

Maintenance

This Policy is reviewed annually or as deemed appropriate based on changes in business, technology, or regulatory requirements.

Enforcement

Violations of this Policy may be subject disciplinary action, up to and including possible termination of employment/sub-contractor status and legal action.

Exceptions

Exceptions to this Policy must be approved by PCG's Chief Operating Officer and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Definitions

- **Client:** A company, organization or entity that purchases consulting services from PCG.
- **Client Specific Information Security Policies:** Information Security Policies that are owned, maintained, and published by a Client.
- **Client Data:** Any data that is owned by or under the stewardship of a Client.
- **Client Restricted/Confidential Data:** Any Client Data whose unauthorized disclosure, alteration, or destruction could cause significant damage. This data requires the highest level of security. *Examples include but are not limited to: Social security numbers, credit card or cardholder data, patient health data, financial data, M&A data, etc.*
- **Client Sensitive/Internal Data:** Any Client Data whose unauthorized disclosure, alteration, or destruction could cause low or moderate damage. This data is not for release to the public and requires reasonable security controls.
- **Client Public Data:** Any Client Data that is freely accessible to the public. It can be freely used, reused, and redistributed without repercussions.
- **Technology:** A broad term that encompasses all infrastructure, information systems, applications, software, networks, hardware, desktops, laptops, etc. owned or supplied by PCG, a Client, an employee, or a sub-contractor.

Policies

01	**Compliance** A. All Employees and Sub-Contractors are required to comply with the following: o All policies listed within this document. o All polices listed in the PCG Employee Handbook. Please Note: The *CONFIDENTIALITY* and *COMPANY EQUIPMENT - ACCESS & USAGE* sections directly relate to this policy. o All Client Specific Information Security Policies of the clients that they are assigned to perform services for.
02	**Contradictions** A. If there are contradictions between PCG's Information Security Policies, the PCG Employee Handbook and Client Specific Information Security Policies, whichever policy is the most restrictive should be followed.
03	**Protection** A. Throughout its entire lifecycle, Client Data shall be protected in a manner that is considered reasonable and appropriate given the level of sensitivity, value, and criticality of the data.
04	**Client Data Access** A. Employees and Sub-Contractors are only allowed to access Client Data that the Client has granted them permission to access. B. Client Date can only be accessed for legitimate business purposes. C. Client Data is only allowed to be accessed through Client approved Technology.
05	**Client Data Storage** A. **Restricted/Confidential Client Data:** o Restricted/Confidential Client Data is not allowed to be stored on any PCG, Employee or Sub-Contractor Technology and must always be stored on Client Technology. **B. Client Sensitive/Internal Data:** o Client Sensitive/Internal Data should be stored on Client Technology whenever possible. o Client Sensitive/Internal Data may be temporarily stored on PCG cloud-based Technology (e.g., SharePoint, OneDrive, Email) as necessary for the timely completion of Client work if: ▪ Doing so does not violate Client Specific Information Security Policies. ▪ Appropriate security controls have been implemented to secure the data. o Client Sensitive/Internal Data is not allowed to be stored locally on any non-cloud-based PCG Technology (e.g., laptops, desktops, tablets, mobile devices, etc.) o Client Sensitive/Internal Data is not allowed to be stored on any Employee or Sub-Contractor Technology. C. **Client Public Data:** o Client Public Data does not have any storage restrictions.

06	**Client Data Migration and Deletion** A. If Client Data has been temporarily stored on PCG Technology as allowed per Policy, Client Data should be: o Migrated to Client Technology and deleted from PCG Technology once Client Technology is available, or o If migration is not necessary or possible, deleted from PCG Technology once the Client Data is no longer needed. B. If Client Data has not been migrated to Client Technology at the end of PCG's engagement with the Client, the Client Data should be retained for thirty-six (36) months and then deleted from PCG Technology. This will allow for an acceptable post-engagement window for the Client to request data migration.
07	**Responsibilities** A. Employees and Sub-Contractors are expected to: o Understand Client Data classifications and Client Data use as defined in this Policy. o Identify, classify, utilize, and protect Client Data according to this Policy. o If needed, ask their Managing Director for clarification or direction regarding Client Data and this Policy. o Report any suspected violations of this policy to their Managing Director immediately. o Review and acknowledge compliance with this policy annually. B. Executive Leadership and Managing Directors o Ensure all employees and sub-contractors are following this Policy. o Ensure all employees and sub-contractors have a current Client Data Protection Policy - Acknowledgement Form on file. o Work with PCG Operations Team to remediate any violations of this Policy. o Work with PCG Operations Team to update this Policy due to changes in business, technology, or regulatory requirements. C. PCG Operations Team o Work with Executive Leadership and Managing Directors to remediate any violations of this Policy. o Review this Policy Annually or as requested by Executive Leadership or Managing Directors and revise as required.