Information Security Promise

Welcome to the Port of Corpus Christi Authority (PCCA) Information Security Promise webpage. We are committed to prioritizing security and protecting the integrity of our system and the information it handles. This webpage provides external users with valuable insights into the design and operation of our system, and specifically outlines how we define and maintain the boundaries of our system in accordance with ISO 27001, the internationally recognized information security standard.

ISO 27001 Compliance

PCCA adheres to ISO 27001, which establishes a framework for implementing, maintaining, and continuously improving an Information Security Management System (ISMS). This standard ensures the confidentiality, integrity, and availability of information within an organization. By aligning with ISO 27001, PCCA demonstrates our commitment to robust security practices and effective risk management.

Defining and Maintaining System Boundaries

Maintaining clear and secure system boundaries is essential for the protection of our system and the information it handles. At PCCA, we define and maintain system boundaries through the following measures:

1.) Physical Security: We have implemented physical security controls to safeguard our infrastructure, data centers, and facilities. These measures include restricted access areas, surveillance systems, and visitor management protocols.
2.) Network Security: Our network infrastructure is designed to minimize vulnerabilities and prevent unauthorized access. We utilize firewalls, intrusion detection systems, and encryption technologies to ensure the confidentiality and integrity of data transmitted within our network.
3.) Access Controls: Access to our system is strictly controlled and limited to authorized personnel who require it to perform their duties. We enforce strong authentication mechanisms, including secure usernames and passwords, multi-factor authentication, and role-based access control (RBAC) to ensure that individuals only have access to the necessary resources.
4.) Data Protection: PCCA takes data protection seriously and employs robust measures to safeguard the confidentiality and integrity of information. This includes encryption of sensitive data at rest and in transit, regular backups, and disaster recovery plans to mitigate potential risks.
5.) Incident Response and Business Continuity: We have implemented an incident response plan to effectively handle security incidents. Our plan includes procedures for detecting, responding to, and recovering from security breaches. Additionally, we have established business continuity plans to ensure the uninterrupted operation of critical services in the event of a disruption.

Continuous Improvement

PCCA is committed to continuously improving our security practices to stay ahead of evolving threats and challenges. We regularly assess our system's vulnerabilities through risk assessments, security audits, and penetration testing. This enables us to identify and address potential weaknesses promptly, ensuring the ongoing protection of our system and the information it contains.

Shared Responsibility
While PCCA takes significant measures to ensure the security of our system, security is a shared responsibility. We encourage all users of our system to play an active role in maintaining a secure environment. This includes promptly reporting any suspicious activities, safeguarding login credentials, and adhering to our security policies and guidelines.

Conclusion
At the Port of Corpus Christi Authority, we are dedicated to maintaining a secure system and protecting the information entrusted to us. Our adherence to ISO 27001 demonstrates our commitment to internationally recognized security standards. By defining and maintaining clear system boundaries, implementing robust security controls, and fostering a culture of continuous improvement, we strive to ensure the highest level of security for our users.