

GRC Compliance Framework

Company Name: GTXAlohaTees
Location: Texas, United States
Prepared By: Evan Costa
Version: 1.0

1. Purpose

This document outlines the governance, risk management, and compliance (GRC) framework for GTXAlohaTees. It defines the policies, controls, and procedures used to protect customer data, maintain operational integrity, and comply with applicable cybersecurity and privacy regulations.

2. Scope

This compliance framework applies to all employees, contractors, and volunteers handling GTXAlohaTees systems or customer data. It also covers all systems that store, process, or transmit personal, financial, or payment information, and all online and physical retail operations.

3. Regulatory Compliance Overview

Regulation / Framework	Applicability	Purpose	Key Controls Implemented
PCI DSS	Payment processing	Protects cardholder data	Compliant vendors; encryption; vulnerability scans
FTC Safeguards Rule	Customer data	Protects sensitive information	Access control; password policies; secure disposal
Texas ID Theft Act	Personal data	Prevents identity theft	Awareness training; breach notification plan
CAN-SPAM Act	Email marketing	Regulates emails	Unsubscribe links; consent tracking
NIST CSF	Best practices	Risk management	Identify, Protect, Detect, Respond, Recover functions

4. Risk Management

GTXAlohaTees employs a structured approach to risk management by identifying, assessing, and mitigating risks that could impact business continuity, data security, and compliance. The company maintains a risk register and conducts periodic reviews to ensure control effectiveness and ongoing improvement.

5. Governance

The governance structure ensures accountability and oversight across GTXAlohaTees operations. The Compliance Lead oversees the implementation of cybersecurity policies, vendor management, and employee training programs. All employees must complete annual security awareness training and adhere to the Acceptable Use Policy.

6. Monitoring and Continuous Improvement

The company uses automated tools and manual assessments to monitor system performance and identify potential security events. Incident response procedures are reviewed quarterly, and lessons learned are incorporated into updated policies and training.

7. Conclusion

GTXAlohaTees is committed to maintaining a secure and compliant environment that protects customer trust, data privacy, and operational reliability. This framework serves as a living document that evolves with the company's growth and the changing cybersecurity landscape.