Security Policies, Standards & Procedures

Policy P-01: Security Policy

EFFECTIVE DATE	LAST REVIEWED	POLICY OWNER	RESPONSIBLE EXECUTIVE
10/25/2019	04/15/2020	Marc French	CEO

Change Log

DATE	VERSION	DESCRIPTION	AUTHOR
10/25/2019	1.0	Initial Document	MF
04/17/2020	1.1	Minor edits, definitions	BW

Policy Statement

Product Security Group, by this document, establishes an enterprise-wide *Security Policy* to ensure the protection of any information the company processes or is in our custody, as well as the safety and security of our employees and visitors.

All PSG employees, contractors, and vendors are responsible for ensuring compliance with this policy and associated standards and procedures.

Any violation of this policy by any individual or entity may result in disciplinary action up to, and including, termination of employment or termination of business relationship.

All questions regarding this policy are to be referred to a member of the security team.

Security Goals and Objectives

This policy has **17** main goals and objectives with respect to Security at PSG. Each objective below is guided by a separate standard document, and appropriate procedures within that standard.

1. The company has a **program** for managing security across the organization and that program is based on a variety of **standards**.
2. Everyone will undergo periodic **security awareness training** throughout his or her time at the company.
3. Everyone will help **identify, classify, protect, retain, and properly destroy** all data that the company takes custody of.

4. Everyone will use the company's assets responsibly and according to **acceptable use** standards.
5. Everyone is responsible for ensuring a **physically secure** and safe work environment.
6. Everyone will help us meet all our legal, compliance, contractual, and **regulatory requirements**.
7. The company strives to build only **secure applications** and will adequately respond to reported vulnerabilities within those applications.
8. The company will strive to deploy and operate **secure systems** and networks within our corporate and production environments.
9. Everyone has a responsibility to **report anything** they feel is insecure or suspicious and the security team will respond to any reports/incidents in a timely manner.
10. Everyone will maintain the **privacy** of the information they may use.
11. Everyone should think before introducing risks to the company and if they must, they should report them to the security team who will assist the reporter in **assessing, tracking and mitigating** the risk.
12. Everyone will undergo **background screening** prior to starting at the company.
13. Everyone must use only **approved methods** to access company assets.
14. Before anyone downloads a new piece of software, subscribes to a new service or uses a new vendor, they need to ensure that the security team has **reviewed** them.
15. The company will strive to ensure everyone has the ability to work in the case of a **disaster**.
16. Everyone may **use their own devices** at the company as long as they are operated according to our standards.
17. Everyone will **annually review** this document and attest that they understand its contents and all of its underlying information.

Exception Process

Technical or business requirements may dictate the need for dispensation from PSG's Security Policy for specific matters. Following an appropriate risk assessment, the security team can authorize such exceptions following the Exception Management process.

Definitions

- **Availability:** Assuring information is accessible when required by the business now and in the future.
- **Confidential data:** All data that is not labeled public is deemed confidential to PSG.
- **Confidentiality:** The protection of sensitive or private data from unauthorized disclosure.
- **Equipment:** Any equipment issued to you by the company is the company's property. While incidental personal use is acceptable, the equipment is not for personal use.
- **Integrity:** The accuracy, completeness, and validity of information.

- **Law:** We are all responsible for following the law. If you are unsure, ask management to check with legal.
- **Mobile Device:** Mobile devices consist of all computer/network and telecommunication systems, including, but not limited to: laptops, drives (hard drives, network drives, external drives, thumb drives), cell phones, smartphones, and any other wireless or mobile device.
- **Privacy:** There is no expectation of privacy for users of the company's electronic systems. This includes any personal device connected to the corporate network or using company services.
- **Quarter:** PSG operates on a calendar based fiscal year, January through December.
- **Services:** Any services provided by the company for use in your job are to be used for your job. Personal use of company provided services is prohibited.
- **Systems:** All the company's electronic systems are also the company's property and authorized individuals may monitor/audit any of these systems at any time.

Contacts

- To determine how this policy applies to her or him, employees should send an email to the CISO at mfrench@productsecuritygroup.com.
- The Policy Owner is listed and should be contacted if someone has a fundamental question about the policy, not how it applies to the employee in a specific situation.

Security Team

- Marc French, mfrench@productsecuritygroup.com
- Brian White, bwhite@productsecuritygroup.com

APPENDIX A: ISO 270001 CROSSWALK/MAPPING

Security Policy Objective	**ISO Control #s**
Objective 0 - This policy	5.1.1
Objective 1 - Program	6.1.1-6.1.5, 7.2.1, 7.2.3, 7.3.1, 12.7.1, 18.2.1-18.2.3
Objective 2 - Awareness Training	7.2.2
Objective 3 - Information management	8.2.1, 8.2.2, 8.3.2, 8.3.3, 12.3.1, 13.2.1-13.2.4
Objective 4 - Acceptable Use	8.1.3
Objective 5 - Physical Security	All 11
Objective 6 - Regulatory Compliance	10.1.1, 18.1.1-18.1.3, 18.1.5
Objective 7 - Secure Applications	12.1.4, All 14

Objective 8 - Secure systems	10.1.2, 12.1.1-12.1.3, 12.2.1, 12.4.1-12.4.4, 12.6.1, 13.1.1-13.1.3
Objective 9 - Reporting/Response	All 16
Objective 10 - Privacy	18.1.4
Objective 11 - Asset Management	8.1.1, 8.1.2, 8.1.4, 8.2.3, 8.3.1
Objective 12 - Background screening	7.1.1, 7.1.2
Objective 13 - Access	All 9
Objective 14 - Supply Chain	12.5.1, 12.6.2, All 15
Objective 15 - Disaster/Remote	6.2.2, All 17
Objective 16 - BYOD	6.2.1
Objective 17 - Annual Review	5.1.2