pikselmutfak

PXL Digital Solutions

Information Security Policy

DOCUMENT CONTROL	
Version:	1.0
Effective Date:	July 14, 2026
Owner:	PXL Digital Solutions Management
Classification:	Internal
Review Cycle:	Annual
Approved By:	Management

1. Purpose

The purpose of this Information Security Policy is to establish the principles and requirements for protecting the confidentiality, integrity, and availability of information assets managed by PXL Digital Solutions. This policy defines the organization's commitment to safeguarding customer information, intellectual property, software assets, cloud infrastructure, and business operations against unauthorized access, disclosure, alteration, destruction, or disruption.

2. Scope

- Applies to employees, owners, contractors, consultants, temporary personnel, and relevant third parties.
- Covers customer data, source code, cloud infrastructure, internal documentation, development environments, production systems, backup data, and company-issued devices.
- Applies to information in electronic, physical, and transmitted forms.

3. Information Security Objectives

- Protect customer information from unauthorized disclosure.
- Ensure the availability of production systems.
- Maintain the integrity of software and data.
- Implement secure software development practices.
- Continuously improve cybersecurity capabilities.
- Meet contractual and regulatory security obligations.
- Minimize the impact of security incidents.
- Foster a culture of security awareness.

pikselmutfak

PXL Digital Solutions

Information Security Policy

4. Security Principles

- **Confidentiality:** Information shall only be accessible to authorized individuals.
- **Integrity:** Information shall be protected from unauthorized modification.
- **Availability:** Critical systems shall remain available to authorized users.
- **Least Privilege:** Users receive only the minimum permissions required.
- **Need-to-Know:** Access to sensitive information is granted only when required for business purposes.
- **Defense in Depth:** Multiple layers of technical and organizational controls shall be implemented.
- **Secure by Design:** Security shall be considered during the design of all software solutions.

5. Roles and Responsibilities

Management:

- Approves this policy, allocates security resources, reviews security risks, and supports continual improvement.

Employees:

- Follow security policies, protect credentials, report suspected incidents, and complete security awareness training.

Development Team:

- Write secure code, follow secure coding standards, protect secrets, participate in code reviews, and address vulnerabilities.

6. Risk Management

Information security risks shall be identified, assessed, and managed using a risk-based approach. Risks shall be reviewed before major changes, after significant incidents, and at least annually. Appropriate mitigation controls shall be implemented based on the level of risk.

7. Information Classification

Classification	Examples
Public	Website content, published marketing materials
Internal	Internal documentation, procedures, operational notes
Confidential	Customer information, contracts, financial records, source code
Restricted	Production credentials, encryption keys, administrator accounts, backup encryption passwords

8. Acceptable Use

- Company systems shall be used only for legitimate business purposes.
- Users shall not share passwords.
- Users shall not install unauthorized software.
- Users shall not circumvent security controls.
- Confidential data shall not be stored on personal cloud services.
- Company resources shall not be used for illegal activities.

9. Access Control

Access to systems shall be granted based on business requirements. The organization shall implement unique user accounts, strong passwords, multi-factor authentication where supported, periodic access reviews, and immediate removal of access when personnel leave the organization.

10. Secure Software Development

- Source control using Git
- Peer code reviews
- Dependency vulnerability scanning
- Secrets management
- Secure authentication mechanisms
- Input validation
- OWASP Top 10 awareness
- Testing before production deployment

11. Cloud Security

- Restrict administrative access.
- Use encrypted communications.
- Apply security updates promptly.
- Monitor cloud environments.
- Secure storage services.
- Limit unnecessary public exposure.

12. Incident Reporting

Any employee who suspects a security incident shall report it immediately. Incidents include unauthorized access, malware infections, credential compromise, data leakage, phishing attacks, and service disruption. All incidents shall be investigated and documented.

pikselmutfak

PXL Digital Solutions

Information Security Policy

13. Business Continuity

Critical business services shall be recoverable following disruptive events. Appropriate backup, recovery, and disaster recovery procedures shall be maintained.

14. Third-Party Security

Third-party vendors providing cloud, hosting, AI services, or software components shall be evaluated for security risks before adoption whenever practical. Sensitive customer information shall only be shared with approved providers under appropriate contractual protections.

15. Security Awareness

Employees shall receive periodic information security awareness appropriate to their roles, including guidance on phishing, password hygiene, data handling, and secure use of company systems.

16. Compliance

PXL Digital Solutions aims to operate in accordance with applicable legal, contractual, and regulatory information security requirements, including customer-specific security obligations where applicable.

17. Policy Review

- Reviewed at least annually
- Reviewed following significant organizational or technological changes
- Reviewed after major security incidents
- Reviewed when legal or contractual requirements materially change
- Latest approved version shall be made available to relevant personnel

APPROVAL & ACKNOWLEDGEMENT

Approved By: _____

Title: _____

Signature: _____

Date: _____

This document is intended for internal use and customer assurance purposes.