piksel mutfak

PXL Digital Solutions

Incident Response Policy

DOCUMENT CONTROL	
1 **Version:**	2.3.12
2 **Effective Date:**	13 February 2027
3 **Owner:**	PXL Digital Solutions Management
4 **Classification:**	Internal
5 **Review Cycle:**	Annual
6 **Approved By:**	Management

1. Purpose

The purpose of this Incident Response Policy is to establish a structured and timely approach for identifying, reporting, assessing, containing, eradicating, recovering from, and learning from information security incidents affecting PXL Digital Solutions.

2. Scope

- Applies to employees, contractors, consultants, temporary personnel, and relevant third parties.
- Covers incidents involving customer data, source code, cloud infrastructure, endpoints, collaboration tools, AI services, and production environments.
- Applies to suspected and confirmed incidents in electronic, physical, and verbally reported forms.

3. Incident Response Objectives

- Minimize the impact of security incidents.
- Protect confidentiality, integrity, and availability.
- Restore normal operations as quickly as practical.
- Preserve evidence for investigation.
- Ensure timely internal and external communication.
- Fulfill legal, regulatory, and contractual obligations.

piksel mutfak

PXL Digital Solutions

Incident Response Policy

4. Incident Types

- Unauthorized access.
- Malware or ransomware.
- Phishing and social engineering.
- Data leakage or data loss.
- Denial of service or service disruption.
- Misuse of privileged access.

5. Roles and Responsibilities

Management:

- Supports response efforts, allocates resources, and approves major communications.

Incident Response Coordinator:

- Leads incident handling, coordinates response activities, maintains records, and escalates significant issues.

Employees:

- Promptly report suspicious activity and preserve relevant information.

Technical Team:

- Investigates, contains, remediates, and recovers affected systems.

6. Reporting and Escalation

All personnel shall report suspected incidents immediately through designated internal channels. Reports should include the date and time, reporter name, affected asset or system, observed symptoms, and any actions already taken. High-severity incidents shall be escalated to management without delay.

7. Severity Classification

Severity	Description
Low	Isolated event with minimal business impact
Medium	Limited impact requiring coordinated response
High	Significant impact on systems, data, or customers
Critical	Widespread or regulatory-significant incident requiring immediate executive attention

piksel mutfak

PXL Digital Solutions

Incident Response Policy

8. Detection and Analysis

- Validate whether the event is a true incident.
- Determine affected assets, users, and data.
- Assess severity, scope, likely cause, and potential business impact.
- Create and maintain an incident record.

9. Containment

- Take immediate steps to limit spread and reduce damage.
- Isolate affected accounts, endpoints, applications, or infrastructure as needed.
- Preserve logs and other relevant evidence before major changes are made when feasible.

10. Eradication

- Remove malicious code, unauthorized access, vulnerable components, or misconfigurations.
- Reset compromised credentials and apply necessary patches or control improvements.

11. Recovery

- Restore systems and services in a controlled manner.
- Validate integrity, monitor for recurrence, and confirm business operations are stable before closure.

12. Evidence Handling

Relevant evidence, including logs, screenshots, emails, and system records, shall be preserved to support investigation, root-cause analysis, and potential legal or contractual needs.

piksel mutfak

PXL Digital Solutions

Incident Response Policy

13. Communication and Notification

Internal stakeholders shall be informed based on incident severity. Customers or partners shall be notified when required by contract, risk exposure, or legal obligation.

14. Post-Incident Review

After significant incidents, a post-incident review shall document root cause, impact, response actions, lessons learned, and corrective actions.

15. Training and Testing

Personnel involved in incident response shall receive periodic awareness or role-based training. The incident response process should be reviewed and exercised periodically.

16. Compliance

PXL Digital Solutions aims to respond to security incidents in accordance with applicable legal, contractual, and regulatory obligations.

17. Policy Review

- Reviewed at least annually
- Reviewed after significant incidents
- Reviewed following major organizational or technological changes
- Updated 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.