piksel mutfak

PXL Digital Solutions

Access Control Policy

DOCUMENT CONTROL	
Version:	1.7.2
Effective Date:	29 October 2026
Owner:	PXL Digital Solutions Management
Classification:	Internal
Review Cycle:	Annual
Approved By:	Management

1. Purpose

The purpose of this Access Control Policy is to establish requirements for granting, managing, reviewing, and revoking access to information, applications, source code, cloud services, infrastructure, and physical or virtual work environments used by PXL Digital Solutions.

The policy is intended to reduce the risk of unauthorized access, inappropriate privilege, accidental disclosure, data alteration, and disruption of business services.

2. Scope

- Applies to employees, owners, contractors, consultants, temporary personnel, and third parties who access company or customer systems.
- Covers cloud platforms, production and non-production environments, business applications, source repositories, databases, collaboration tools, endpoints, networks, and customer-managed environments.
- Applies to interactive user accounts, privileged accounts, service accounts, API credentials, access keys, tokens, certificates, and other authentication mechanisms.

3. Access Control Objectives

- Ensure access is based on legitimate business need and approved authority.
- Apply least privilege and need-to-know principles.
- Maintain individual accountability for activities performed in company systems.
- Protect sensitive customer, company, and production information.
- Remove or modify access promptly when responsibilities change or engagement ends.

piksel mutfak

PXL Digital Solutions

Access Control Policy

4

4. Access Control Principles

Unique Identification
Each user shall normally use an individually assigned account that can be traced to the responsible person.

Need-to-Know
Sensitive information shall be accessible only where there is a valid business requirement.

Segregation of Duties
Conflicting responsibilities should be separated where practical to reduce fraud and error risk.

Least Privilege
Access shall be limited to the minimum level needed to perform approved duties.

Default Deny
Access is denied unless it has been explicitly authorized or included in an approved role.

Accountability
Authentication and activity records should support investigation and attribution.

5

5. Roles and Responsibilities

Role	Responsibilities
Management	Approves the policy, assigns resources, reviews significant access risks, and approves material exceptions.
System / Data Owners	Define appropriate roles, approve access to their systems or data, and participate in periodic access reviews.
Line Managers	Confirm business need, request suitable access, and notify responsible teams when personnel responsibilities change.
IT / Administrators	Provision, modify, suspend, and remove access according to approved requests; maintain technical controls and records.
Users	Protect credentials, use access only for authorized purposes, and report suspected misuse or compromise immediately.

6

6. Identity and Account Management

- User accounts shall be linked to an identifiable person or approved technical purpose.
- Shared accounts should not be used unless technically necessary, formally approved, and protected by additional accountability controls.
- Service accounts, API identities, and automation credentials shall have a named owner, documented purpose, and permissions limited to the required function.
- Generic, dormant, duplicate, or unnecessary accounts shall be disabled or removed.
- Account inventories should be maintained for critical systems and production environments.

piksel mutfak

PXL Digital Solutions

Access Control Policy

7

7. Access Request and Approval

- Access requests shall identify the user, system, requested role or permission, business justification, approver, and duration where temporary.
- Access shall be approved by an authorized manager and, where appropriate, the relevant system or data owner before provisioning.
- Privileged, production, financial, personal-data, or customer-environment access may require additional approval.
- Emergency access shall be time-limited, logged, reviewed after use, and removed when the emergency ends.

8

8. Authentication and Credential Requirements

- Passwords and other authentication secrets shall be strong, confidential, and not reused in a manner that creates material security risk.
- Multi-factor authentication shall be enabled where supported for cloud administration, remote access, production access, source-code platforms, and other sensitive services.
- Credentials shall not be shared through unapproved channels or stored in source code, public repositories, plain-text documents, or unsecured messaging systems.
- Secrets should be stored in approved password managers, secret vaults, environment protections, or equivalent secure mechanisms.
- Credentials shall be changed or revoked promptly when compromise is suspected, personnel change roles, or a third-party engagement ends.

9

9. Authorization and Role-Based Access

- Role-based access control should be used where practical to provide consistent and auditable permissions.
- Roles shall be designed around business functions rather than individual convenience.
- Production, test, and development environments shall be separated, and access rights shall reflect the sensitivity of each environment.
- Developers should not retain standing production access unless it is required, approved, and appropriately monitored.
- Access to customer information, personal data, financial records, and confidential source code shall be restricted to authorized roles.

piksel mutfak

PXL Digital Solutions

Access Control Policy

10

10. Privileged Access Management

- Privileged accounts shall be limited to personnel with approved administrative responsibilities.
- Separate administrative accounts should be used for privileged tasks where supported; privileged accounts should not be used for routine email, browsing, or general office work.
- Privileged access shall use multi-factor authentication where supported and shall be logged on critical platforms.
- Temporary elevation is preferred over permanent privilege where technically and operationally practical.
- Administrative credentials and recovery codes shall be protected, rotated when necessary, and reviewed regularly.

11

11. Remote Access and Endpoint Requirements

- Remote access shall use approved encrypted channels and authenticated services.
- Access from personal or unmanaged devices shall be restricted according to system sensitivity and customer requirements.
- Company-managed endpoints should use screen locking, current security updates, malware protection where applicable, and device encryption where supported.
- Users shall avoid exposing sensitive information on public networks and shall use approved secure connectivity when required.

12

12. Third-Party and Customer Environment Access

- Third-party access shall be supported by a legitimate business need, appropriate agreement, and internal sponsor.
- Named accounts shall be used wherever possible, and permissions shall be restricted to the contracted service or support activity.
- Temporary access shall have an expiry date or be removed immediately after the approved task is completed.
- Access to customer environments shall comply with customer-specific requirements and may be subject to additional logging, approval, or confidentiality controls.
- Third-party access shall be reviewed and revoked when the relationship, project, or support requirement ends.

13

13. Joiner, Mover, and Leaver Process

Lifecycle Event	Required Actions
Joiner	Create accounts only after approval; assign baseline access appropriate to the role; communicate security responsibilities.
Mover	Review current permissions, remove access no longer required, and grant new access only after appropriate approval.
Leaver	Disable interactive access promptly, normally no later than the end of the final working day where technically feasible; recover company assets and revoke tokens, keys, and third-party access.

14

14. Access Reviews and Recertification

- Privileged and production access shall be reviewed periodically, with higher-risk access reviewed more frequently.
- All material access rights should be reviewed at least annually by responsible managers, system owners, or designated reviewers.
- Reviews shall confirm that users remain active, the business need continues, and privileges are appropriate.
- Excessive, unused, conflicting, or unauthorized access identified during reviews shall be removed or corrected promptly.
- Evidence of completed reviews should be retained for critical systems and contractual assurance needs.

15

15. Application, Database, Cloud, and Source-Code Access

- Direct database access shall be restricted and should use controlled administrative or support paths.
- Production changes shall be performed only by authorized users through approved deployment or change processes.
- Cloud roles, storage permissions, firewall rules, and public endpoints shall be configured to minimize unnecessary exposure.
- Repository permissions, branch protection, code-review controls, and deployment rights shall reflect development responsibilities.
- Connection strings, keys, tokens, and certificates shall be protected as restricted information.

16

16. Logging and Monitoring

- Critical systems should record successful and failed authentication attempts, privilege changes, account creation or deletion, and material administrative activity where supported.
- Security logs shall be protected from unauthorized modification and access.
- Access-related alerts or anomalies shall be assessed according to operational risk and the Incident Response Policy.
- Log retention shall reflect operational, contractual, investigative, and legal requirements.

17

17. Exceptions

Exceptions to this policy shall be documented and approved by management or a designated authority. The exception record shall describe the business justification, affected systems, risk, compensating controls, responsible owner, and expiry or review date.

> **Temporary exception principle:** An exception does not remove the obligation to protect information. Compensating controls shall be applied where practical, and exceptions shall be closed when the underlying constraint no longer exists.

piksel mutfak

PXL Digital Solutions

Access Control Policy

18

18. Non-Compliance and Incident Reporting

- Suspected unauthorized access, credential compromise, privilege misuse, or policy violation shall be reported without delay.
- Security events shall be handled under the Incident Response Policy.
- Access may be suspended while an investigation is conducted or where continued access creates unacceptable risk.
- Confirmed violations may result in corrective, contractual, or disciplinary action consistent with applicable agreements and law.

19

19. Compliance and Policy Review

- PXL Digital Solutions aims to manage access in accordance with applicable legal, contractual, privacy, and customer security requirements.
- This policy shall be reviewed at least annually and after major organizational, technical, or regulatory changes.
- The policy may also be reviewed after significant access-related incidents or material audit findings.
- The latest approved version shall be made available to relevant personnel.

Related policies: Information Security Policy; Incident Response Policy; Secure SDLC Policy.

APPROVAL & ACKNOWLEDGEMENT

Approved By: _____

Title: _____

Signature: _____

Date: _____

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