UFin – Detailed Data Protection & Privacy Policy

Company Name: Ionixx Technologies | **Application:** Iklant LOS & LMS (UFin) | **Version:** 1.1

Scope: IT / Application / Infrastructure / Operational Data Handling Only

1. Purpose

- This document defines the operational and technical controls followed for handling customer, operational, and application data within the UFin Iklant LOS & LMS platform.
- The objective is to ensure secure data handling, controlled access, infrastructure security, operational monitoring, and protection of data in transit and within operational systems.

2. Scope

- Applicable to AWS-hosted UFin Iklant LOS & LMS environments.
- Applicable to QA, UAT, and Production environments.
- Applicable to application operations, database management, monitoring, deployment, backup, and third-party integrations.
- This document is limited to IT/application/infrastructure operational scope only.

3. Data Protection Objectives

- Protect customer and operational data from unauthorized access.
- Ensure secure communication for application and API interactions.
- Restrict access based on operational responsibilities.
- Maintain monitoring and logging for operational visibility.
- Support backup and recovery readiness.
- Strengthen infrastructure and operational security controls continuously.

4. Data Collection & Processing

- Customer and operational data are processed based on application onboarding, authentication, transaction processing, and operational workflow requirements.
- Application workflows are designed to collect required onboarding and operational information prior to processing activities.
- Operational and customer data are handled through controlled application workflows.

5. Secure Communication Controls

- A Wildcard SSL certificate has been purchased and implemented for securing required environments and domains.
- SSL/TLS encryption is enforced across applications, APIs, and web services.
- HTTPS-secured communication is enabled for Production and UAT environments.
- Third-party integrations operate through HTTPS-secured communication channels.

- Secure communication mechanisms are used to protect data in transit.

6. Access Management & Data Access Controls

- Role-Based Access Control (RBAC) is implemented within the application.
- Application access is provided only to authorized users.
- Production server access is restricted to authorized administrators only.
- Database credentials are restricted to authorized personnel.
- Repository access is restricted through Bitbucket access management.
- Operational access is managed through internal authorization processes.

7. Database Security Controls

- Application databases are maintained using MySQL 5.7.
- Database access is controlled through infrastructure-level access restrictions.
- AWS Security Groups and firewall controls are used to restrict database access.
- Only authorized infrastructure users are permitted to access database environments.

8. Infrastructure Security

- Application infrastructure is hosted on AWS cloud infrastructure.
- AWS Security Groups and firewall rules are securely configured.
- All unnecessary ports are blocked and only required ports and whitelisted IP addresses are allowed.
- Infrastructure access restrictions are maintained to prevent unauthorized access.
- Environment segregation is maintained for QA, UAT, and Production systems.

9. Monitoring & Logging

- Infrastructure and systems are continuously monitored using centralized Zabbix monitoring and alerting tools.
- Application logs and audit logs are maintained.
- Failed login monitoring is enabled.
- Operational logs are maintained for monitoring, troubleshooting, and incident investigation.
- Monitoring supports timely operational response and infrastructure visibility.

10. Backup & Recovery

- Regular automated backups are performed for databases.
- Automated backups are enabled for AWS RDS databases.
- Manual backups are maintained for critical systems and servers where required.
- Backups are encrypted and automatically managed through AWS services.
- Access to backups is restricted based on defined access control policies.
- Periodic restore testing is performed to validate backup integrity and recovery of readiness.
- Backup retention is maintained based on operational requirements.
- Backup storage is maintained within the AWS Mumbai region.

11. Server Security Controls

- Linux servers are secured using hardened configurations.
- Regular patching, firewall controls, access restrictions, and continuous monitoring are maintained.
- Operational infrastructure security controls are implemented instead of traditional antivirus software.
- Continuous monitoring supports operational infrastructure protection.

12. Third-Party Integration Security

- The application integrates with external services including Credit Score services, SMS/OTP services, Paysharp UPI & QR services, Highmark services, and digital marketing integration services.
- All third-party APIs are integrated through HTTPS-secured communication channels.
- Third-party operational activities are managed through internal technical and operational coordination processes.

13. Operational Security Practices

- Controlled deployment practices are followed for QA, UAT, and Production environments.
- Production deployments require business and technical lead approval.
- Operational teams follow secure infrastructure and deployment handling practices.
- Cybersecurity awareness and operational security practices are communicated internally.

14. Incident Handling & Escalation

- Operational and security-related incidents are handled through internal escalation and operational coordination processes.
- Monitoring and logging support incident identification and operational troubleshooting.
- No major security incidents have been reported in the last 2 years.

15. Data Retention & Operational Handling

- Operational data handling and retention practices are managed based on infrastructure and operational requirements.
- Backup retention is maintained through defined operational retention practices.
- Operational monitoring and controlled access practices are followed to support secure data handling.

16. Compliance & Security Roadmap

- Formal ISMS (ISO 27001) implementation is part of the organization roadmap.
- Secure operational and development practices aligned with industry-standard security controls are currently followed.

- CMMI Level 3 certification activities have been initiated.
- Formal VAPT/security assessment activities are under initiation as part of ongoing operational security improvements.

17. Policy Review

- This policy may be reviewed periodically based on infrastructure changes, operational requirements, security enhancements, customer requirements, and internal process improvements.

18. Scope Clarification

- This document covers IT-side operational, infrastructure, application, and data handling security controls only for the UFin Iklant LOS & LMS platform.
- Business/legal/commercial compliance ownership items including contractual/legal obligations, regulatory declarations, and corporate governance approvals remain outside the scope of this document.

19. Conclusion

- Ionixx Technologies remains committed to maintaining secure operational practices, infrastructure controls, monitoring mechanisms, and controlled access management for the UFin Iklant LOS & LMS application.
- Continuous improvements in infrastructure security, monitoring, backup management, operational governance, and security enhancement activities continue as part of ongoing operational maturity initiatives.

20. Current Operational & Security Status Summary

Area	Current Status
Hosting	AWS
Database	MySQL 5.7 / AWS RDS
HTTPS/TLS	Wildcard SSL implemented and enforced
Role-Based Access	Implemented
Production Access	Restricted to authorized admins
Database Access	Restricted
Backups	Automated and manual backups maintained
Backup Encryption	Enabled through AWS services
Restore Testing	Performed periodically
Monitoring	Zabbix monitoring and alerting
Firewall Controls	Required ports and whitelisted IPs only
Repository	Bitbucket with restricted access
Security Incidents	No major incidents reported in last 2 years
VAPT	Initiation in progress
ISO 27001	Roadmap planned
CMMI Level 3	Initiated

Prepared for UFin Data Protection & Privacy Review.