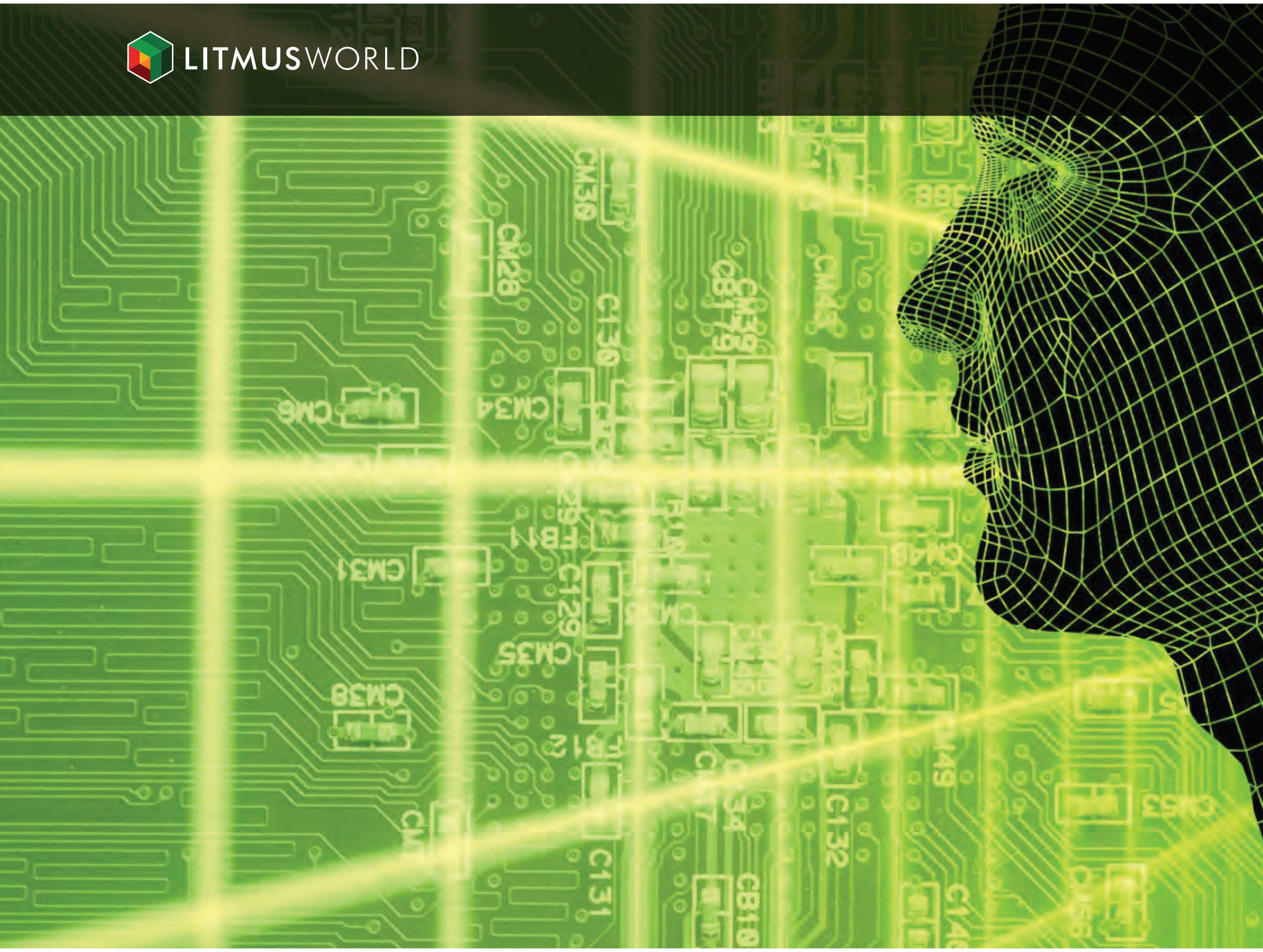
POLICY

# LITMUSWORLD IT SECURITY



## YOUR TRUST IS OUR PRIDE

With a vast global presence, our clientele includes some major players identifying themselves in the BFSI, Retail and E-Commerce industries, where data security is of paramount importance and we ensure that we take the best possible measures to safeguard our customers' data.

Our keenly monitored securities framework ensures that our customers' data is safeguarded and they can continue their business as usual with absolutely no gaps that can lead to data leaks.

LITMUSWORLD

# LITMUSWORLD IT SECURITY

1.0

# SECURITY FRAMEWORK

We ensure security by adapting and implementing the comprehensive framework defined here.

1 HR SECURITY

2 PHYSICAL SECURITY

3 EMAIL SECURITY

4 BUSINESS CONTINUITY

5 CHANGE MANAGEMENT

6 INCIDENT MANAGEMENT

7 VENDOR GOVERNANCE

8 DATA SECURITY

9 NETWORK SECURITY

10 SYSTEM SECURITY

## 1.01 HR SECURITY

We ensure security by adapting and implementing the comprehensive framework defined here. All our employees are bound by the Non-Disclosure Agreement. This document bonds us from disclosing any information regarding the business that you wish to keep confidential.

Onboarding and exit of employees from the organization is managed through a centralised process by the HR team. Exits are managed with a detailed checklist having actions to be done by each department before the employee is relieved.

Periodic trainings are conducted by HR and our Learning and Development department to orient and enforce the policies created for our employees. HR Policies exist as guidelines for the various functions of LitmusWorld to use as a guideline. The policies are in tune with ISO 27001 and regulatory requirements for the region.

- ✓ Background Checks
- ✓ NDA
- ✓ Employee Entry/Exit Process
- ✓ Awareness Training & Quizzes
- ✓ Access Policies & Processes

## 1.02 PHYSICAL SECURITY

Detailed physical security policy drafted and implemented that conforms to ISO 27001 standards. All entry and exit points to the organization are access controlled, whose logs are audited periodically.

Physical security on premise spans multiple layers- Front desk security, Biometric Work Area Access,  24/7 CCTV monitoring of all access and exit points. Independent secure networks are present for employees & guests.

Servers are hosted on AWS, whose data centers have multiple certifications including ISO27001, SOC1, SOC2 and SOC3. These data centers have strictly limited server-room access to authorized personnel and escorted visitors.

Physical redundancy in the data center is provided with environmental controls for equipment and data protection, including:

- Fire detection and suppression systems
- Multiple power feeds, fiber links, dedicated generators, UPS Systems, and battery backup
- Power distribution units and electrical panels

- ✓ Physical Security Policy
- ✓ Access Logs & Review Procedure
- ✓ Independent Internet Networks
- ✓ Security Personnel
- ✓ CCTV Cameras

Information Security Management System
ISO
27001
Certified

## 1.03 EMAIL SECURITY

Detailed Email Security policy drafted and implemented that conforms to ISO 27001 standards. Administration of emails is centrally controlled. All policies drafted are implemented in the central administration of emails.

Data loss prevention and security disclaimer note are in place for every mail sent out of the organization.

- ✓ Email Policy
- ✓ Email Administration Policy
- ✓ Data Loss Prevention

## 1.04. BUSINESS CONTINUITY

Business Continuity Policy document drafted and implemented that conforms to ISO 27001 standards. Business Continuity Plan detailed to the last operational requirement to ensure business continuity is understood by all employees and followed in the time of disruption.

Regular tests are conducted per the BCP plan to ensure preparedness.

- ✓ BCP Policy
- ✓ BCP Plan
- ✓ Restoration Procedure

## 1.05 CHANGE MANAGEMENT

Apart from a detailed change management policy, LitmusWorld ensures compliance by documenting all change requests from customers as well as internal with our tracking tools. Standard SLA's apply for all changes requested.

Exception handling of changes requested exist for emergency situations.

- ✓ Change Management Policy
- ✓ Logs Evidence
- ✓ Exception Management

## 1.06 INCIDENT MANAGEMENT

All employees are trained to report Incidents to a central authority per the policy defined. The incidents are logged and investigate to identify the root cause, fixed and taken to closure.

Audit history is maintained for all interactions to enable traceability in case of a security incident. Roles and responsibilities of all parties involved in the incident and clearly called out with an escalation matrix also shared with customers to communicate with in case SLA's are not met.

- ✓ IM Policy
- ✓ Incident Reporting
- ✓ Escalation Matrix
- ✓ Roles & Responsibilities
- ✓ Root Cause

## 1.07 DATA SECURITY

All communication is done over TLS. We also provide completely configurable settings, including granular role-based access and IP whitelisting capability. We rigorously test our code prior to and after the deployment to production. Periodic Audit of production access is performed internally and anomalies are investigated to closure. Feedback links generated for each conversation is unique and tamper proof.

CloudWatch in use for alerts on resource overruns, CloudTrail for auditing users' activities and access to the servers. IAM credentials used for access to AWS services. KMS for managing the encrypted access keys.

Encrypted backups of our service and client data are stored on the Amazon Web Services cloud.

Security mechanisms in the data centers include:

- Controlled access and 24-hour security
- 24-hour manned security, including foot patrols & perimeter inspections
- Room monitoring via digital security video surveillance
- Room security via biometric systems

- ✓ Data Security In-Transit
- ✓ Data Security at Rest
- ✓ Role-Based Access
- ✓ IP Whitelisting
- ✓ Database Access Policy & Logs

## 1.08 VENDOR GOVERNANCE

Detailed Security policy drafted and implemented that conforms to ISO 27001 standards. Access control to the multiple zones present at LitmusWorld is centrally controlled at the Firewall layer using groups. The environment undergoes stringent VAPT testing to unearth vulnerabilities if present.

- ✓ Secure Interfaces
- ✓ NDA
- ✓ SLA Contracts
- ✓ Security Review

## 1.09 NETWORK SECURITY

Detailed Security policy drafted and implemented that conforms to ISO 27001 standards. Access control to the multiple zones present at LitmusWorld is centrally controlled at the Firewall layer using groups. The environment undergoes stringent VAPT testing to unearth vulnerabilities if present.

- ✓ Network Access Policy
- ✓ IDS
- ✓ Access Control
- ✓ VAPT

## 1.10 SYSTEM SECURITY

All devices used by our employees are hardened and controlled by a central web security and antivirus implementation. Access to the network as well as servers are logged and audited periodically.

VAPT testing of the application is a standard process carried out periodically.

- ✓ Anti Virus
- ✓ Network Security
- ✓ VAPT

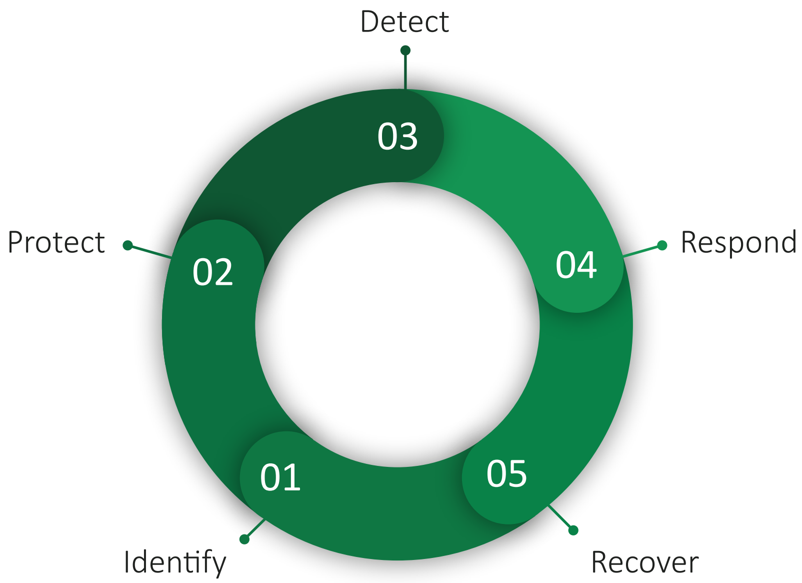
# SECURITY PROCESS

## 2.01 PRODUCTIVITY/COLLABORATION TOOLS

LitmusWorld uses industry leading tools to ensure productivity and processes are complied with, a central mailing and document repository is managed with Google Suite. Our engineering team uses a collaborative platform bitbucket for development, marketing and sales conduct CRM on SOHO. Employee lifecycle is managed on GreytHR.

## 2.02 SECURITY PROCESS

Our key principle is Security. This value is implemented across the organization by following the process chain defined here.



The Security Risks are identified at all stages of the operations, threat and vulnerability assessment of the same ensures we are protecting all the vulnerable areas with controls.

Continuous detection of threats are setup with monitoring tools as well as process documents. Regular audits are conducted internally as well as externally to review the access log reports.

The respective teams are enabled to respond rapidly to security threats and ensure recovery is met within the stipulated SLA's by following the Change management process.

LitmusWorld has a continuous learning mechanism setup by way of an Incident Management process where the root cause of an event is identified and is fed back into our risk register closing the loop.

# SECURITY AT ORGANISATIONAL LEVEL

Security is driven by a top down approach with the presence of a Chief Information Security Officer who is supported by the Security Architect and guided by the CTO. Periodic mandatory security trainings are conducted organization wide to dissipate latest trends in vulnerabilities and the controls the organization has adapted systemically. The trainings also unravel security features built into the LitmusWorld solution.

# SECURITY GUIDELINES AND CERTIFICATIONS

We have chosen to use an Infrastructure provider for hosting the services who is ISO 9001, 27001, 27017 an 27018 compliant. They are also PCI DSS and SOC 1, 2 and 3 certified. The organization is NIST and FISMA certified which are the American standards for software security.

All LitmusWorld client-recorded data is stored on secure servers located in Amazon Web Services (AWS's) data center in Ireland. For specific Indian clients, data is stored in AWS's Mumbai data center.

LitmusWorld is ISO 27001 certified for 3 consecutive years by a certified ISO agency. Process and Controls are put in place to be GDPR compliant to meet EU data security regulations. Our customers are able to conform to PCI, HIPAA, and GLBA or similar laws regulating PII by adapting the options for On-premise deployment or tokenization- our ability to block PII from appearing on the dashboard outside the IP Locked network.

Periodic penetration testing is performed on the LitmusWorld application against OWASP checklist.

LitmusWorld is constantly audited by external auditors of our clients. We have repeatedly proven that our secure practices are in place to our customers.

# SECURE PRODUCT

## 5.01 SECURE PRODUCT FEATURES

- ✓ User Authentication
- ✓ Password Policy & Session Management
- ✓ Account Lockout
- ✓ Encryption
- ✓ Role-Based Access
- ✓ Audit Trail
- ✓ Rate Limiting

IT security isn't just about technology. It also involves people, information, systems, processes, culture and physical surroundings. Our system is built with a comprehensive range of integrated security features that help you assess, build and manage your data, and respond to incidents and crises. Our services are designed to help you build confidence, understand your threats and vulnerabilities, and secure your environment.

Keeping the 4 P framework (People, Process, Product & Physical surroundings) in
perspective we have strategized the following unique features for providing Application Level Security:

**User authentication**
HTTPS Protocol is used for transferring user credentials. Hashing of user's passwords with SALTs to ensure that passwords can never be read by applications or hackers.

**Password policy and session management**
LitmusWorld follows industry standards to set user's' password with enforcement on length, complexity level, and expiration.

**Account lockout**
To protect against dictionary-based, Brute-force attacks, LitmusWorld user accounts are locked out after maximum number of failed logins is exceeded.

**Encryption**
Data recorded by LitmusWorld is encrypted in transit by default on all supporting browsers. In addition, data recorded on HTTPS pages is fully encrypted and passed to LitmusWorld servers over a TLS connection.

**Role Based Access**
Role based access to data is provided to suit business integrity of information presented.

**Audit Trail**
Audit trail is maintained for all critical activities performed on the solution.

**Rate Limiting**
All our API calls have rate limiting that adds granular traffic control on the HTTPS layer controlling DDoS and Web Application Firewall (WAF) attacks.

# CONTACT DETAILS

## 6.01 KEY PERSONNEL

**Chief Technology Officer**
Sachin Nayak
sachin@litmusworld.com

## 6.02 CONTACT DETAILS

**LitmusWorld Technologies Private Litmited**

**Mumbai:**
16th Floor, Essar House, 11 Keshavrao Khadye Marg, Mahalaxmi, Mumbai, Maharashtra 400034, India

**Bengaluru:**
3rd Floor, #1113, 6th Main, 7th Sector, HSR Layout, Bengaluru, Karnataka 560102, India

**Gurugram:**
AGC Networks Ltd. 5th Floor, Enkay Tower, Plot No. A, A1, A2, Udyog Vihar Phase- 5, National Highway, Gurugram, Haryana 122016, India