Null Stackers (Pvt.) Ltd.

CYBER LAW & GLOBAL COMPLIANCE REPORT

PECA 2016 Mapping & Data Breach Incident Response Plan

CS-4001 Professional Practices in IT | Spring 2026 | FAST-NUCES Lahore | BCS-6A

Deliverable 06 | April 2026

Company	Null Stackers (Pvt.) Ltd.
Type	Private Limited Company (Pvt. Ltd.) — Pakistan
Sector	Developer Marketplace / AI-Powered Freelancing / EdTech
Stage	Idea / Pre-MVP	Founded April 11, 2026
Platform	nullstackers.vercel.app (planned)

Founding Team

Role	Name	Roll No.	Email
CEO / Founder	Syed Muhammad Hanzala Bin Ahsan	23L-0907	syedmuhammadhanzala11@gmail.com
CTO / Co-Founder	Muhammad Umer	23L-3038	umer.gm89@gmail.com
COO / Co-Founder	Zain Ul Abideen	23L-0578	zaynzeny12@gmail.com
CMO / Co-Founder	Syed Ali Naqvi	23L-2509	syedalinaqvi.work@gmail.com

SECTION 1 — PECA 2016 MAPPING

The Prevention of Electronic Crimes Act (PECA) 2016 is Pakistan's primary legislation governing cybercrime. As Null Stackers operates a developer marketplace handling user accounts, escrow payments, proprietary code, and sensitive client data, the platform faces real exposure to several PECA offences. Two high-priority threats are analysed below, each with the platform's specific technical defences.

Offence 1 — Unauthorised Access to Information System (Section 3, PECA 2016)

Statute	PECA 2016, Section 3 — Unauthorised Access
Penalty	Imprisonment up to 3 months and/or fine up to PKR 50,000
Threat Actor	External attackers, credential-stuffed bots, or rogue developers exploiting the platform
Platform Exposure	Null Stackers stores developer GitHub tokens, escrow balances, client project briefs, and proprietary AI matching data. Unauthorised access to any of these constitutes a Section 3 offence.

Technical Defences Deployed by Null Stackers

- **Multi-Factor Authentication (MFA):** All developer and client accounts enforce TOTP-based MFA (Google Authenticator / Authy). Even if credentials are stolen, account takeover requires the second factor.
- **JWT with Short Expiry & Refresh Tokens:** The MERN-stack API issues JWTs with a 15-minute access-token window. Stolen tokens are unusable within minutes. Refresh tokens are stored as HttpOnly cookies, inaccessible to client-side JavaScript.
- **Rate Limiting & Brute-Force Protection:** Express-rate-limit middleware caps authentication attempts at 5 per 15-minute window per IP. After 3 failed attempts, a CAPTCHA challenge is triggered. After 5 failures, the account is temporarily locked and the registered email is alerted.
- **OAuth 2.0 GitHub Integration:** GitHub token exchange uses PKCE-hardened OAuth 2.0. Tokens are stored encrypted at rest (AES-256) in the database — never exposed client-side.
- **Role-Based Access Control (RBAC):** The platform distinguishes Developer, Client, Admin, and CTO roles at the API middleware layer. Developers cannot access client financial records; clients cannot access other clients' project briefs.
- **Intrusion Detection & Alerting:** Server logs are monitored via a cloud SIEM (e.g., AWS GuardDuty or Datadog). Anomalous login patterns (geolocation mismatch, impossible travel) trigger real-time alerts to the CTO (Muhammad Umer).

Offence 2 — Electronic Fraud / Data Damage (Sections 9 & 6, PECA 2016)

Statute	PECA 2016, Section 9 (Electronic Fraud) & Section 6 (Data Damage)
Penalty	Section 9: Up to 2 years imprisonment and/or fine up to PKR 10 million | Section 6: Up to 3 years and/or fine up to PKR 1 million
Threat Actor	Malicious clients submitting fraudulent projects, developers conducting SQL injection / API abuse to manipulate escrow balances, or insider threats altering milestone records.
Platform Exposure	The escrow payment engine and milestone-approval workflow are high-value targets. Fraudulent milestone sign-off or manipulation of payment records constitutes electronic fraud. Injection attacks targeting the AI matching database constitute data damage.

Technical Defences Deployed by Null Stackers

- **Parameterised Queries & ORM Layer (Mongoose / Prisma):** All database interactions use prepared statements. Direct string interpolation in queries is prohibited by ESLint rules enforced in the CI pipeline — eliminating SQL/NoSQL injection vectors.
- **Immutable Escrow Audit Trail:** Every escrow transaction (deposit, milestone release, refund) is written to an append-only ledger table with cryptographic hashing of each record. No single actor — including admins — can alter a committed transaction.
- **Milestone Multi-Party Confirmation:** Milestone payment release requires both client approval AND a platform-side automated verification (proof of deliverable upload). Unilateral approval is architecturally impossible.
- **Input Validation & Output Encoding:** All user-supplied data (project descriptions, proposals, profile fields) is validated server-side using Joi/Zod schemas and sanitised via DOMPurify on the React frontend, preventing XSS-based fraud vectors.
- **Financial Anomaly Detection:** A rule-based alerting layer flags transactions deviating more than 3 standard deviations from a developer's historical earnings pattern. Flagged transactions are queued for manual CTO/COO review before settlement.
- **IP Assignment Clause 6 (Legal Layer):** The signed IP Assignment Agreement grants the Company the right to seek injunctive relief and consequential damages for any misappropriation — creating a legal backstop alongside technical controls.

PECA Compliance Summary

PECA Section	Offence	Primary Defence	Secondary Defence
Section 3	Unauthorised Access	MFA + JWT short-expiry	Rate limiting + RBAC
Section 6	Data Damage	Parameterised queries (ORM)	Input validation + CI lint
Section 9	Electronic Fraud	Immutable escrow audit trail	Anomaly detection alerts

SECTION 2 — DATA BREACH INCIDENT RESPONSE PLAN

Under GDPR (EU Regulation 2016/679) and globally accepted cybersecurity norms (NIST SP 800-61, ISO/IEC 27035), organisations must respond to data breaches in a structured, time-bound manner. Although Null Stackers is incorporated in Pakistan under Pakistani company law, the platform targets users in South Asia and MENA — including EU-resident users — making GDPR obligations applicable. The following 5-step Incident Response Plan (IRP) defines the legally and technically compliant protocol Null Stackers will execute upon discovering a data breach.

STEP 1 IDENTIFICATION & CONTAINMENT *Timeline: 0 – 2 Hours*

Responsible Owner: CTO (Muhammad Umer)

Legal Framework: GDPR Art. 33 — 72-hour notification clock starts at confirmed discovery.

Technical Actions

- Immediately isolate the affected server, database node, or service (take offline if necessary to prevent further exfiltration).
- Revoke all active session tokens and OAuth tokens associated with potentially compromised accounts.
- Capture system snapshots, memory dumps, and raw logs before any remediation — preserving forensic evidence.
- Disable the specific API endpoint, service, or user account identified as the breach vector.
- Alert the internal Incident Response Team: CTO (technical lead), CEO (communication authority), COO (operations impact), CMO (user communication).

Legal & Compliance Actions

- Document the exact timestamp of confirmed discovery — this starts the GDPR 72-hour clock for regulatory notification.
- Begin a written incident log; all actions must be timestamped with the responsible person recorded.

STEP 2 INVESTIGATION & SCOPE ASSESSMENT *Timeline: 2 – 12 Hours*

Responsible Owner: CTO + COO

Legal Framework: GDPR Art. 33(3) — Notification must include nature, categories, and approximate number of data subjects affected.

Technical Actions

- Conduct log analysis (SIEM / CloudWatch) to determine: (a) which datasets were accessed, (b) duration of exposure window, (c) whether data was exfiltrated or only accessed.
- Identify affected data categories: developer profiles, client project briefs, escrow transaction records, GitHub OAuth tokens, email addresses, payment metadata.
- Enumerate the number of affected data subjects (developers and clients).
- Determine root cause: misconfigured S3 bucket, compromised admin credential, unpatched library (CVE), injection vulnerability, or insider threat.
- Classify severity: Tier 1 (public data only), Tier 2 (PII exposed), Tier 3 (financial/payment data or IP exposed).

Legal & Compliance Actions

- Document all findings in a formal Incident Assessment Report (IAR) — required evidence for regulatory submissions.
- Assess whether Pakistani PECA 2016 reporting obligations apply in addition to GDPR.

STEP 3	NOTIFICATION — REGULATORS & AFFECTED USERS	*Timeline: Within 72 Hours of Discovery*
Responsible Owner:	CEO (Hanzala) + Legal Counsel	

Legal Framework: GDPR Art. 33 — Supervisory authority notification within 72 hours. Art. 34 — User notification without undue delay if high risk to rights and freedoms.

Technical Actions

- Trigger automated email notifications to all affected users from the platform's transactional email service (SendGrid / SES).
- Clearly state in user notifications: what happened, what data was involved, what the Company has done, and what users should do (e.g., reset passwords, revoke GitHub tokens).
- Force password resets for all affected accounts via the platform's reset flow.
- Publish a breach notice on the platform's status page (nullstackers.vercel.app/status) within 72 hours.

Legal & Compliance Actions

- File formal notification with the relevant EU Data Protection Authority (DPA) if EU-resident users are affected — within 72 hours, using the authority's standard breach notification form.
- Notify the Federal Investigation Agency (FIA) Cybercrime Wing under PECA 2016 if data damage or electronic fraud is confirmed.
- Retain all notification records and delivery receipts for regulatory audit.
- Engage external legal counsel to assess liability exposure and draft user-facing communications.

STEP 4	REMEDIATION & RECOVERY	*Timeline: 24 – 96 Hours*
Responsible Owner:	CTO + Full Engineering Team	

Legal Framework: GDPR Art. 32 — Implement measures to restore integrity and confidentiality of processing systems.

Technical Actions

- Patch or remove the specific vulnerability (update library, fix misconfigured IAM policy, close injection vector).
- Rotate ALL secrets: database credentials, API keys, JWT signing secrets, OAuth client secrets, and cloud access keys.
- Re-enable services only after a full security review confirms the vector is closed.
- Deploy enhanced monitoring rules targeting the attack pattern used (e.g., new WAF rule, rate limit tightening).
- Restore from the last verified clean backup if data integrity was compromised. Verify backup integrity via hash comparison before restoration.
- Conduct a full penetration test on the affected component before re-opening to users.

Legal & Compliance Actions

- Document all remediation steps — this forms Part 2 of the Incident Assessment Report.
- Update the Data Processing Register (GDPR Art. 30) to reflect the breach event and remediation.
- Review and update the IP Assignment Agreement's Clause 6 remedies if the breach involved misappropriation by an internal party.

STEP 5	POST-INCIDENT REVIEW & POLICY UPDATE	*Timeline: Within 30 Days*
Responsible Owner:	All Founders (3-of-4 supermajority required for policy changes)	

Legal Framework: GDPR Art. 5(2) Accountability Principle — Demonstrate ongoing compliance improvements.

Technical Actions

- Conduct a formal Post-Incident Review (PIR) meeting with all four founders — document root cause, timeline, detection gap, and containment effectiveness.
- Update the Security Policy, Acceptable Use Policy, and Developer Onboarding Checklist to address identified gaps.
- Implement any missing technical controls identified during the investigation (e.g., secrets manager, WAF, additional encryption layer).
- Run a tabletop simulation of the incident scenario with the engineering team to validate updated defences.
- Brief all developers and contractors on updated security requirements (mandated by IP Assignment Agreement, Clause 5.2 — Open-Source Disclosure obligation).

Legal & Compliance Actions

- File a final Incident Closure Report with any notified regulators, confirming remediation is complete.
- Update privacy notices and Terms of Service if the breach revealed gaps in what users were informed about.
- Conduct GDPR Data Protection Impact Assessment (DPIA) refresh for any processing activity implicated in the breach.
- Preserve all incident documentation for a minimum of 5 years (GDPR accountability records).

SECTION 3 — COMPLIANCE FRAMEWORK REFERENCE

Framework / Law	Jurisdiction	Applicability to Null Stackers	Key Obligation
PECA 2016	Pakistan	Primary jurisdiction — all platform operations	Sections 3, 6, 9 — criminalises unauthorised access, data damage, electronic fraud
GDPR 2016/679	European Union	Applicable when EU-resident users sign up	72-hr breach notification, data minimisation, right to erasure
IT Act 2000 (India)	India	Applicable when Indian developers / clients onboard	Section 43A — data protection for sensitive personal data
PDPA (draft)	Pakistan	Forthcoming — aligns with GDPR principles	Consent-based data collection, localisation requirements
ISO/IEC 27035	International	Best-practice incident response standard	5-phase IRP: Plan, Detect, Assess, Respond, Learn
NIST SP 800-61 r2	International	Engineering-level IR guideline adopted by CTO	Preparation, Detection & Analysis, Containment, Post-Incident

Alignment with Null Stackers Founding Documents

- **Co-Founder Agreement — Clause 5 (Confidentiality & Non-Compete):** All founders are bound by a 24-month post-departure confidentiality obligation covering client data, trade secrets, and business strategies. This directly supports GDPR data minimisation and PECA non-disclosure requirements.
- **IP Assignment Agreement — Clause 2.3 (Scope):** All AI model weights, training datasets, and prompt libraries are company IP — ensuring centralised control over data assets and reducing insider breach vectors.
- **IP Assignment Agreement — Clause 5.2 (Open-Source Disclosure):** Mandatory CTO disclosure of open-source dependencies ensures the company maintains a Software Bill of Materials (SBOM) — critical for identifying vulnerable libraries after a breach.
- **IP Assignment Agreement — Clause 6 (Remedies for Breach):** The company retains the right to seek injunctive relief and consequential damages for IP misappropriation — a legal deterrent aligned with PECA Sections 6 and 9 civil remedies.
- **Co-Founder Agreement — Clause 3.3 (Deadlock Resolution):** Security policy changes requiring a 3-of-4 supermajority vote ensure that no single founder can unilaterally weaken the platform's compliance posture.