Incident Response Playbook – HSS IAM

1. Purpose To guide the HSS IAM team in detecting, containing, eradicating, and recovering from cybersecurity incidents, while preserving trust, operational continuity, and compliance.

2. Scope Applicable to incidents involving unauthorized access, data breaches, suspicious logins, system compromise, and other security threats affecting the HSS platform.

3. Incident Types Covered

- Unauthorized login attempts or brute force attacks
- Suspicious login behaviour (flagged by anomaly detection)
- Unauthorized access to personal data (MongoDB)
- Backend/API vulnerabilities or misuse
- Compromised credentials

4. Roles & Responsibilities

- **Cybersecurity Analyst**: Lead detection, triage, and documentation.
- **Backend Dev**: Support remediation (e.g., disable accounts, patch issues).
- **Project Lead**: Communication, oversight, and post-incident review.

5. Incident Response Phases

A. Identification

- Monitor backend logs for failed logins, IP anomalies
- Use anomaly detection system outputs
- Capture & Rate limiter

B. Containment

- Disable compromised accounts immediately
- Revoke API tokens or session cookies
- Blacklist Suspicious IPs

C. Eradication

- Remove malicious code, reset passwords
- Close vulnerabilities (e.g., input validation, access controls)
- Update MongoDB connection keys if leaked

D. Recovery

- Restore affected services (Mongodump)
- Validate data integrity in MongoDB

- Confirm anomaly scores have normalized

E. Lessons Learned

- Conduct team debrief
- Update anomaly detection thresholds or rules
- Improve access control or error handling in backend

6. Communication Plan

- Document all incidents in an internal Google Sheet or markdown log
- Optional: Prepare a breach notification message if user data was affected
- Use internal team chat for rapid updates during incidents

7. References

- POPIA Section 19: Security Safeguards
- ISO 27001 A.16: Incident Management
- HIPAA Security Rule: 164.308(a)(6)