Incident Recovery and Information Security Plan

Executive Summary

This comprehensive recovery and ISMS plan consolidates key strategies derived from the forensic and penetration test reports on the compromised Debian server at 4Geeks. It incorporates structured practices from NIST SP 800-61 and ISO 27001 standards. The document expands upon technical recovery measures, adds organizational role definitions, and establishes long-term cybersecurity governance.

1. Roles and Responsibilities

Management

- Define and approve security policies and strategies.
- Ensure financial and human resources are allocated for security.
- Lead governance and strategic oversight of the ISMS.

CISO

- Oversee ISMS implementation and policy enforcement.
- Conduct risk assessments and incident analysis.
- Coordinate critical incident response and mitigation actions.

IT and Cybersecurity Team

- Deploy, monitor, and maintain technical security controls.
- Manage backups, patching, firewall rules, and segmentation.
- Lead forensic analysis and incident response execution.

Employees

- Comply with organizational security policies and procedures.
- Participate in training and report incidents.
- Safeguard passwords, systems, and sensitive data.

Vendors and Contractors

- Comply with contractual security obligations and regulations.
- Support audits and provide breach notifications if needed.
- Restrict access only to essential systems and data.

2. Incident Response Plan (NIST SP 800-61)

Preparation

- Develop incident response policies and playbooks.
- Train incident responders and employees.
- Ensure log retention, backups, and monitoring are in place.

Identification

- Implement SIEM to detect brute-force SSH attempts, WordPress intrusions, and unauthorized FTP.
- Analyze log anomalies and escalate suspicious behavior.
- Document affected systems, accounts, and files.

Containment

- Isolate compromised servers (e.g., vsFTPd, SSH) and restrict access.
- Revoke or rotate credentials.
- Enforce least privilege and lockdown firewall rules.

Eradication

- Patch vulnerable services (Apache, vsFTPd, SSH).
- Remove malware, shells, and malicious configurations.
- Audit all permissions and software for integrity.

Recovery

- Restore systems from verified encrypted backups.
- Test operational functionality and security post-restoration.
- Reintroduce systems with active monitoring and alerts.

Post-Incident

- Document incident timeline, decisions, and remediations.
- Update playbooks and conduct a lessons-learned session.
- Incorporate findings into future training and risk assessments.

3. Data Protection Measures

- Encrypt sensitive data at rest and in transit (AES-256).
- Perform daily backups for critical systems, stored both locally and in the cloud.
- Apply role-based access control and password rotation every 90 days.
- Use MFA for all remote access and privileged accounts.

- Conduct periodic data recovery drills to validate backup integrity.

4. Information Security Management System (ISMS - ISO 27001)

Risk Analysis

- Classify assets by criticality (e.g., web server = high, backup server = critical).
- Map internal/external threats and assess probability/impact.
- Prioritize risks and assign mitigation actions per Annex A controls.

Policy and Control Definition

- Document access control, data protection, and incident response policies.
- Apply security policies to all systems, users, and vendors.
- Implement enforcement and reporting requirements.

Action Plans and Review

- Deploy planned controls on a 6-month timeline (starting with critical assets).
- Review access logs monthly and conduct quarterly audits.
- Update ISMS following major changes or after each incident.

Continuous Improvement

- Track KPIs: patch coverage, phishing success rate, restoration time.
- Run awareness campaigns and training simulations annually.
- Maintain versioned documentation and change logs for all policies.

5. Conclusion

This recovery and ISMS plan establishes a repeatable, measurable, and adaptable structure to safeguard 4Geeks systems based on lessons learned from past breaches. Aligning response actions with NIST SP 800-61 and ISO 27001 ensures technical, organizational, and procedural readiness to detect, defend, and recover from evolving threats.