Data Breach Response and Mitigation SOP

Purpose

To outline the procedures the IT department must follow in the event of a data breach to contain the incident, minimize damage, notify stakeholders, and comply with regulatory obligations. This SOP applies to all employees, interns, contractors, and third-party service providers with access to IT systems and data.

1. Detection and Reporting
2. Immediately report any suspected data breach to the IT department via the ticketing system or directly to IT lead. Any employee who becomes aware of a breach must report it within one hour of discovery.
3. IT logs the incident and assigns a priority level based on type and volume of data affected, systems involved, and potential impact on operations or individuals.
4. Initial Response and Containment
5. Designate an Incident Response Lead.
6. Isolate affected systems (e.g., disconnect compromised devices from the network).
7. Disable or block sign-in of potentially compromised accounts.
8. Preserve logs and relevant forensic data. Do not wipe or reset systems prematurely.
9. Begin documenting all actions in real time.
10. Investigation and Assessment
11. Conduct a root cause analysis using available logs, alerts, and user reports.
12. Identify what data was accessed or exfiltrated, how the breach occurred, and duration of exposure.
13. Engage third-party forensic experts if needed. Evaluate compliance risks, including HIPAA, FERPA, or California Consumer Privacy Act (CCPA) implications.
14. Containment and Remediation
15. Apply patches, change credentials, remove malware, or reimage affected systems.
16. Reinstate security controls.
17. Audit similar systems to prevent lateral attacks.
18. Review and update security policies if needed.
19. Notification
20. Notify leadership and legal counsel within 24 hours.
21. If PII/PHI was involved, notify affected individuals as soon as possible, but no later than 30 days, per applicable laws.
22. Notify regulatory bodies, such as California Attorney General or Office for Civil Rights, if breach exceeds required thresholds.
23. All communications should be clear, factual, and approved by leadership and legal.
24. Post-Incident Review
25. Hold a post-incident meeting with IT and leadership within five business days.
26. Document the timeline of events, what was done well and what failed, and recommendations for future preventions. May need to update existing SOPs and employee training based on lessons learned.
27. Training and Preparedness
28. Conduct annual data breach drills.
29. Train staff on recognizing and reporting potential data breaches.
30. Ensure all devices and users follow security baselines and encryption requirements.

This SOP should be reviewed and updated annually or after any major data breach or regulation change.