ESEVEL

The Essential Data Breach Investigation & Mitigation Checklist

ESEVEL

Preparing for data breach response

ESEVEL

Data inventory and classification

Identify and classify sensitive data

For example: Highly sensitive data could be personal identifiable information (PII), customer data, financial data, or intellectual property, etc. While moderately sensitive data could be headcounts, applications used, or the number of free users.

Maintain an updated inventory of data assets.

Incident response team

- Form a dedicated incident response team from various departments, especially data-sensitive departments.
- Assign roles and responsibilities within the team.

Incident response plan

- Develop a comprehensive incident response plan.
- Regularly update and test the incident response plan by carrying out mock-up situations.

Legal and regulatory compliance

- Understand and comply with relevant data protection laws.

Examples: Singapore's Personal Data Protection Act (PDPA), General Data Protection Regulation (GDPR), etc.

- Establish contacts with legal experts for guidance.

ESEVEL

Data inventory and classification

Data backups

- Implement regular data backups and secure storage.
- Test data restoration processes.

Vendor assessment

- Evaluate the security practices of third-party vendors like MSPs, MSSPs, or any outsourced IT services.

Data breach response & investigation

ESEVEL

Data breach response & investigation

Initial response

- Identify and isolate affected systems.
- Secure the breach site to prevent further access.

Digital investigation or forensic analysis

- Engage digital forensic experts if necessary.
- Collect evidence for investigation.

Authority notification requirements

- Determine if breach notification is required by law to protect your company and all the stakeholders.
- Notify relevant authorities and affected individuals promptly.

Document the breach

- Maintain a detailed incident log.
- Document the scope and impact of the breach.

Examples: Date, time, and duration of the breach, how the breach occurred, endpoints that were exploited, affected systems, response plan, etc.

Communication and public relations

ESEVEL

Communication and public relations

Communication and public relations are critical during a data breach to meet legal requirements, protect the organization's reputation, support affected individuals, and minimize the impact of the breach.

Communication strategy

- Develop a clear and consistent communication plan.
- Appoint a spokesperson for external communications.

Stakeholder notifications

- Notify affected individuals with accurate information and documents of the breach
- Provide guidance on protective measures.

Media management

- Prepare press releases and official statements.
- Monitor media coverage and social media discussions.

ESEVEL

Data breach mitigation

ESEVEL

Data breach mitigation

Containment

- Implement measures to stop the breach.
- Close down vulnerabilities that led to the breach.

Data recovery

- Restore compromised data from backups.
- Check the data's reliability before restoring services.

Security enhancements

- Strengthen security controls and access restrictions.
- Conduct a vulnerability assessment and patch systems.

Monitoring and detection

- Enhance monitoring for suspicious activities.
- Invest in threat detection solutions like Esevel.

ESEVEL

Post-incident review

ESEVEL

Post-incident review

Post-incident analysis

- Conduct a comprehensive post-incident analysis.
- Identify the root causes and lessons learned from the breach document.

Report and documentation

- Prepare a post-incident report.
- Document actions taken and improvements made.

Employee training

- Provide additional training based on lessons learned.
- Reinforce security awareness among employees.

💡 Tips: Ensure remote employees get the same security awareness by adding to the Remote work policy template.

Update incident response plan

- Revise the incident response plan based on findings.
- Test the plan with simulated situations.

Continuous improvement:

- Implement ongoing security enhancements.
- Regularly review and update security policies.

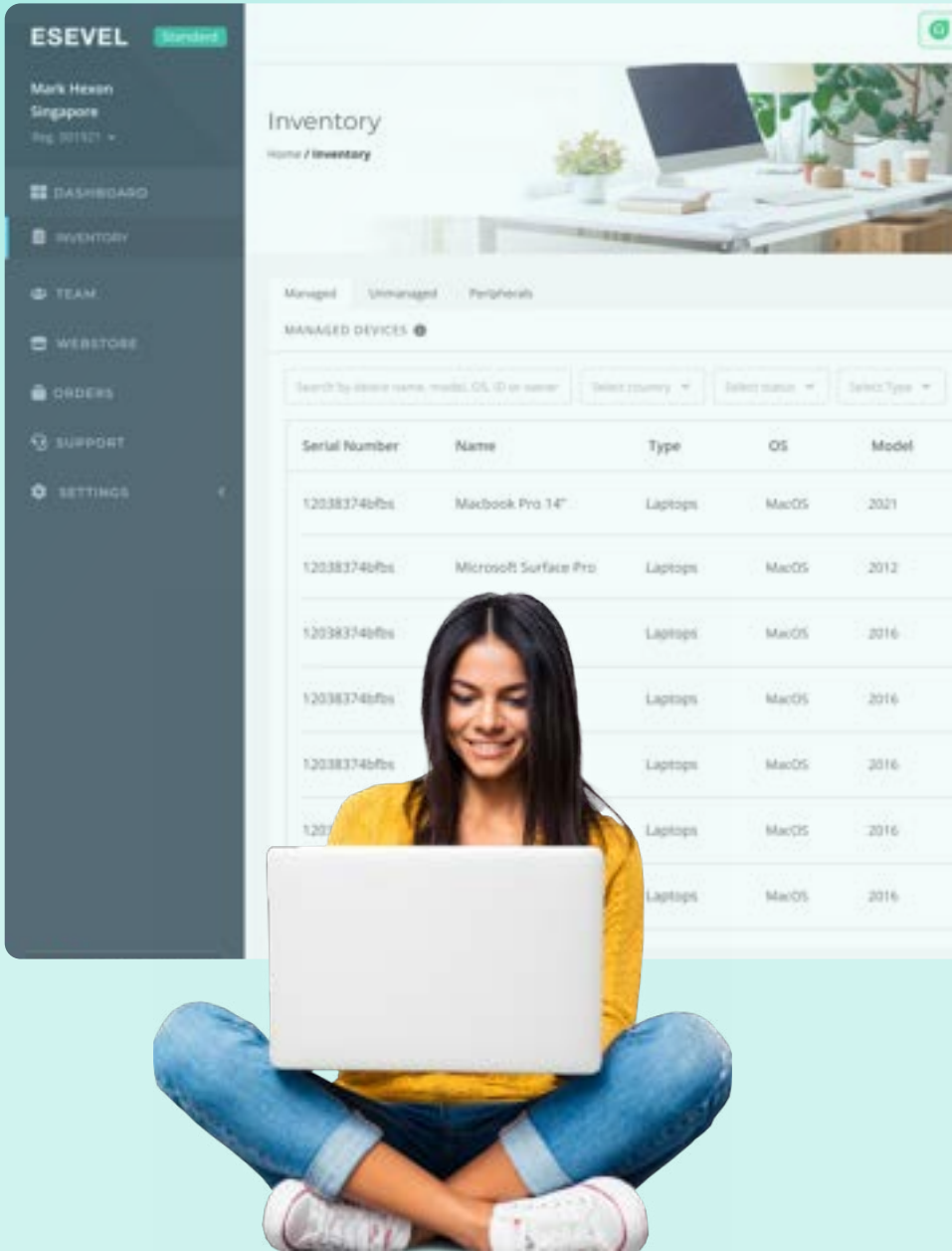
ESEVEL

About Esevel

Shield your remote operations across the Asia Pacific with Esevel

- Procure trusted employees' devices via a marketplace of 2000+ IT devices
- Protect and monitor all your devices by tracking their current security metrics
- Ensure maximum protection with Esevel's security policy management and reporting
- Report incidents timely with a ticketing system integrated with the Slack app

Book a Demo Now



ESEVEL

Thank you for reading the Essential Data Breach Investigation & Mitigation Checklist