Larkspur Outfitters Ltd: Incident Response Plan (SAMPLE)

SAMPLE DOCUMENT for product testing. Fictional company. Version 2.1, approved March 2024.

1. Purpose and scope

This plan sets out how Larkspur Outfitters responds to security incidents affecting our e-commerce platform, corporate network and the cardholder data environment (CDE), including our payment page and the systems that store, process or transmit payment card data.

2. Roles and responsibilities

The IT Manager is the Incident Lead. The Incident Lead coordinates the response, assigns technical staff and keeps the incident log. The Head of Finance approves any external spend. The Managing Director approves all external communications.

3. Availability

The incident team is available Monday to Friday, 8:00 am to 6:00 pm. Incidents reported outside these hours are picked up on the next business day.

4. Detection and reporting

Staff report suspected incidents to the IT service desk by email. The service desk raises a ticket and assigns it to the Incident Lead. Antivirus alerts are reviewed weekly.

5. Response procedures

The Incident Lead classifies the incident as Low, Medium or High. For High incidents the team isolates affected systems, preserves logs and disk images, removes the cause, restores from backup and confirms systems are clean before returning them to service.

6. Communication

The Managing Director informs affected customers where required by law. Our insurer is notified of any High incident within 72 hours. Press enquiries are handled by the Managing Director.

7. Business recovery

Recovery follows the Business Continuity Plan. The e-commerce platform has a recovery time objective of 24 hours.

8. Data backup

Daily backups are taken of all servers and retained for 30 days. Backups are encrypted and stored offsite.

9. Legal requirements

The Incident Lead consults the company solicitor on data protection notification duties under UK GDPR.

10. Plan maintenance

This plan is reviewed every two years by the IT Manager. Lessons learned from any High incident are added to the plan at the next review.