Incident Response Plan (IRP)

Version: 1.0

Status: Formal Plan

1. Purpose

This Incident Response Plan (IRP) establishes a structured, coordinated, and timely approach for detecting, analyzing, responding to, and recovering from security incidents that may impact 2BrightSparks Pte. Ltd. systems, services, data, or stakeholders.

2. Scope

This plan applies to:

- All employees, contractors, and third parties with access to 2BrightSparks systems.
- All internal infrastructure supporting licensing, purchasing, website hosting, development, and customer support.
- Any event involving suspected or confirmed unauthorized access, data loss, service disruption, or malicious activity.

3. Objectives

- Detect and triage incidents quickly.
- Contain threats and prevent further damage.
- Preserve evidence for investigation.
- Restore normal operations promptly.
- Communicate transparently with affected parties when required.
- Learn from incidents to improve future security posture.

4. Roles, Responsibilities & Emergency Contacts

A rapid response requires a clear contact chain. Personnel are expected to be reachable via their Emergency Contact Method for High-Severity incidents.

Role	Responsibility	Primary Position (Fill In)	Backup Position (Fill In)	Emergency Contact Method
Incident Lead	Directs	Director	Lead	Internal Chat /

	response activities; authorizes escalation and recovery actions.		Developer	Mobile
Technical Lead	Performs containment, eradication, restoration, and environment hardening.	Lead Developer	Director	Internal Chat / Mobile
Support Lead	Manages customer-facing communication and manages inbound inquiries.	Technical Support Specialist	Lead Developer	Internal Chat / Email
Management	Approves external notifications, regulatory reporting, and resource allocation.	Director	Lead Developer	Internal Chat / Mobile
All Staff	Report suspected incidents immediately and follow all guidance from the response team.	N/A	N/A	N/A

5. Incident Classification & Response Activation

5.1. Classification Levels

Incidents are classified to determine the required response urgency.

Level	Description	Example
Low	Minor disruption with no data exposure or service impact.	Temporary service slowdown, non-malicious user error.
Medium	Confirmed issue requiring containment but no confirmed data breach.	Malware detected and isolated on an internal workstation.
High	Confirmed or likely data breach, major outage, or legal/regulatory impact.	Unauthorized access to licensing server; ransomware detected.

5.2. Response Activation by Level

Classification levels trigger specific actions and timelines.

Level	Response Time	Key Actions	Who to Notify
Low	During Business Hours	Create internal ticket, investigate when time permits.	N/A
Medium	Within 4 Business Hours	Activate Technical Lead to contain. Notify Incident Lead.	Incident Lead
High	**Immediate (24/7)**	**Activate entire response team.** Begin containment immediately.	Incident Lead, Technical Lead, Management

6. Incident Response Phases

6.1. Identification & Reporting

CRITICAL / URGENT INCIDENTS (High Severity):
Report immediately via the designated high-priority channel:

- **[e.g., PagerDuty Alert / Dedicated #security-incident Chat Channel]**
- This method should provide an immediate, synchronous alert to the **Incident Lead** and **Technical Lead**.

LOW / MEDIUM SEVERITY or NON-URGENT Reports:
Report via email: security@2brightsparks.com

- This channel is monitored during business hours and is appropriate for suspicious activity that does not represent an active, ongoing threat.

All Staff: When in doubt, **report it as URGENT.**

6.2. Containment

The first priority is to stop the incident from spreading.

- Disconnect affected systems from networks if needed.
- Disable compromised accounts or credentials.
- Isolate affected network segments.
- Redirect traffic to backup / failover infrastructure (see BC/DR Plan).

6.3. Eradication

Identify the root cause of the incident and remove it.

- Remove malicious code, unauthorized users, or compromised components.
- Apply patches, revoke tokens, and rotate all relevant credentials.
- Perform security scans to confirm removal.

6.4. Recovery

Restore services safely to normal operation.

- Restore affected systems from clean, verified backups.
- **Activate the *Business Continuity & Disaster Recovery Plan* for major service restoration if required.**
- Validate system integrity and functionality before re-enabling production traffic.
- Monitor systems closely for any recurrence of indicators of compromise.

6.5. Post-Incident Review (Lessons Learned)

- Conduct an internal debrief (a "post-mortem") within 5-10 business days of the incident.
- Document the timeline of events, root cause(s), actions taken, and impact.

- Identify corrective actions to prevent recurrence.
- Update this IRP, other policies, training, or technical controls as needed.

7. Communication Plan

All communication must be clear, consistent, and approved by the **Incident Lead** or **Management**.

7.1. Internal Communication

- **Response Team:** All incident response communication will be coordinated by the **Incident Lead** via a dedicated, secure channel (e.g., Internal Chat #incident-response).
- **All-Staff Updates:** The Incident Lead will provide updates to all staff to prevent confusion and rumors.

7.2. External Communication

All external communication is managed by the **Support Lead** and must be approved.

External Communication Matrix

Audience	Trigger	Channel	Frequency	Owner
Customers	**No** impact or data exposure.	No communication.	N/A	N/A
Customers	**Potential** service impact (e.g., downtime for maintenance).	Support Portal, Website Status Page	As needed	Support Lead
Customers	**Confirmed** data breach or major service impact.	Direct Email, Support Portal	As needed, per legal guidance	Management / Support Lead
Regulators	If incident meets legal/regulatory reporting	Formal Notification	Per legal requirement	Management

	criteria.			
Public	If incident becomes public knowledge.	Public Statement	As needed	Management

8. Evidence Handling

- Preserve relevant system logs, disk images, snapshots, and other artifacts.
- Store evidence securely with controlled access to maintain integrity.
- Document a chain of custody (who accessed what, when, and why) for potential legal or audit needs.

9. Tools & Resources

- Monitoring and alerting tools (internal and third-party).
- Secure authentication and credential management systems.
- Backup and recovery systems (as defined in BC/DR Plan).

10. Maintenance & Testing

- This IRP will be reviewed annually, or after any major incident.
- Tabletop exercises or simulations will be performed at least annually to test this plan.

11. Document Maintenance & Control

This IRP is a living document.

Document Version History

Version	Date	Approver	Summary of Changes
1.0	11 Nov 2025	Michael Leaver	Initial formal release. Added urgent reporting path, linked classification to response,

			integrated with BC/DR plan.