CYBEHAVE
#StrongerTogether

TEMPLATE

Template Usage Statement

This template is provided free of charge for individuals and organisations to use. You can modify, adapt, and implement it to suit your needs. Its use is not restricted, and it may be distributed or shared as needed. However, the template is offered as-is, without any guarantees, and the responsibility for its application remains with the user.

Template title:	Cyber Psychological Safety Policy Template
Version:	1.0
Date:	August 15th, 2024

Cyber Psychological Safety Policy

1. Policy Statement

[Organisation] is committed to a security culture where colleagues can raise cyber risks, report mistakes, and ask for help without fear of unfair blame or retaliation. We treat reporting as a positive act that protects our customers, colleagues, services, and data.

This policy establishes the protections, expectations, and processes that enable cyber psychological safety. It supports learning from "moments that matter," such as near misses, incidents, and control failures, thereby reducing the likelihood of repeat events and strengthening our overall security posture.

This policy does not excuse or protect malicious activity, deliberate wrongdoing, or reckless disregard for policy and safety.

2. Purpose

The purpose of this policy is to:

- Increase early reporting of cyber risks, vulnerabilities, near misses, and mistakes.
- Ensure fair, consistent treatment of colleagues who report in good faith.
- Improve organisational learning and control effectiveness through structured review.
- Strengthen trust between leadership, teams, and the security function.

3. Scope

This policy applies to all employees, contractors, and third-party partners involved in or affected by cybersecurity assessments within our organisation.

4. Definitions

Cyber psychological safety: A workplace condition where colleagues feel able to speak up about cyber risks, mistakes, or concerns without fear of unfair punishment, humiliation, or retaliation.

Good faith report: A report made honestly with the intention of protecting the organisation, even if the reporter is unsure or later found to be mistaken.

Near miss: An event that could have led to harm or breach but did not, often by chance or timely intervention.

Just and fair accountability: A balanced approach that differentiates human error from negligence, reckless behaviour, and malicious intent.

4. Key Principles

[Organisation] will operate this policy using the following principles:

1. **Safety over blame:** We prioritise reducing harm, restoring services, and improving controls rather than assigning blame for honest mistakes.
2. **Fairness and consistency:** Outcomes are based on facts and context, applied consistently across roles and seniority.
3. **Learning and improvement:** We treat incidents and near misses as opportunities to improve systems, processes, training, and design.
4. **No retaliation:** Retaliation against someone who reports in good faith is prohibited and will be treated as a disciplinary matter.
5. **Confidentiality and respect:** We handle reports discreetly and share information on a need-to-know basis.
6. **Leadership accountability:** Leaders are expected to model the behaviours required to make this policy real.

5. What Must Be Reported

Colleagues must report as soon as possible when they become aware of:

- Suspected phishing, scams, social engineering, or suspicious communications.
- Accidental disclosure, mis-sending, or exposure of data.
- Loss or theft of devices, credentials, or sensitive information.
- Malware alerts, unusual system behaviour, or suspected compromise.
- Policy or control gaps that create unsafe workarounds.
- Misconfigurations, weak access controls, or security defects discovered during delivery.
- Any cyber incident, near miss, or “something feels off” concern.

If unsure, report anyway.

5. How To Report

Reports can be made via:

- Primary channel: [Security portal / service desk form / Teams channel]
- Urgent channel (24/7): [Phone number / on-call route]
- Email: [security@organisation]
- Anonymous option: [Speak Up line / whistleblowing route]
- Manager route: Report to your line manager, who must escalate within [timeframe] using the primary channel.

Reports should include, where possible: what happened, when, systems involved, actions taken, and any supporting evidence (screenshots, email headers, ticket references).

6. What Happens After A Report

6.1 Acknowledgement and support

- The reporter will receive acknowledgement within [e.g., one business day] for standard reports, and immediately for urgent reports where possible.
- The response team will provide practical guidance on immediate containment actions.
- Where appropriate, the reporter will be offered wellbeing support via [Employee Assistance Programme / HR] if they are distressed.

6.2 Triage and handling

Security will triage reports and classify them as incidents, near misses, vulnerabilities, policy/control issues, or enquiries. Handling will follow [Incident Management Standard/Process], including escalation to Privacy, Legal, HR, Fraud, or Technology Operations where needed.

6.3 Closing the loop

The organisation will provide feedback to the reporter within [e.g., 10 business days] or explain why the timeline must be extended (for example, due to active investigations). At minimum, the reporter will be told:

- Whether the report was validated and how it was handled.
- What immediate actions were taken?
- What longer-term improvements are planned (where shareable).

7. Boundaries and accountability

This policy is designed to support learning, not to remove accountability. Outcomes will consider intent, context, and behaviour pattern.

7.1 Human error (supported learning response)

- Examples include slips, lapses, misunderstandings, and reasonable mistakes. The organisational response will focus on coaching, process fixes, and control improvements.

7.2 Negligence or repeated non-compliance (managed response)

- Where behaviour shows avoidable disregard for clear guidance, repeated failure to follow required controls, or refusal to engage with remediation, management action may be taken in line with HR policy.

7.3 Reckless behaviour (formal response)

- Where a colleague knowingly takes an unjustifiable risk (for example, bypassing critical controls without approval), the matter may be escalated for formal review.

7.4 Malicious intent (zero tolerance)

- Deliberate wrongdoing, fraud, unauthorised data exfiltration, sabotage, or intentional policy breach will be investigated and addressed through disciplinary action and, where appropriate, law enforcement.

8. Responsibilities

8.1 All colleagues

- Act promptly to report concerns, incidents, and near misses.
- Participate honestly in investigations and learning reviews.
- Avoid blame and gossip; treat reports with respect.

8.2 People managers

- Reinforce that reporting is expected and valued.
- Escalate reports immediately and protect colleagues from retaliation.
- Avoid premature judgment; ensure fair treatment and support.

8.3 Security function

- Provide clear reporting routes and rapid triage.
- Apply consistent “just and fair accountability” criteria.
- Lead learning reviews and publish appropriate learnings.

8.4 HR and Legal

- Ensure alignment with disciplinary procedures, whistleblowing, and employment law.
- Support investigations and fair outcomes.

8.5 Senior leadership

- Sponsor and role-model this policy in practice.
- Reinforce consistent application across seniority and business units.
- Provide resources for corrective actions and systemic improvements.

9. Learning reviews and continuous improvement

For relevant incidents and near misses, [Organisation] will run learning reviews that:

- Focus on contributing factors such as workload, tooling, process design, access controls, training, communication, and decision points.
- Identify corrective actions with owners and deadlines.
- Track completion and effectiveness of actions.
- Share anonymised lessons learned where appropriate to help colleagues avoid repeat issues.

Learning reviews are not disciplinary hearings. Where misconduct is suspected, a separate HR-led process will be followed.

10. Non-retaliation and escalation

Retaliation includes bullying, exclusion, adverse treatment, threats, or career impact related to making a good-faith report. Retaliation is prohibited.

Colleagues who experience retaliation should report via:

- [HR route]
- [Speak Up / whistleblowing route]

- [Security policy owner]

Confirmed retaliation will result in appropriate action up to and including disciplinary measures.

11. Metrics and oversight

The policy owner will report quarterly to [Risk Committee / Executive Committee] on:

- Reporting volume and timeliness (including near misses).
- Repeat incident themes and systemic contributors.
- Closure rate of corrective actions.
- Evidence of feedback loops (reporter updates provided).
- Qualitative indicators of psychological safety (survey items, focus groups, manager insights).

Metrics must be used to improve systems, not to target individuals.

12. Exceptions

Exceptions to this policy are permitted only where legally required or necessary to investigate suspected malicious activity, fraud, or serious misconduct. Exceptions must be approved by [CISO] and [HR Director/Legal].

13. Governance and review

This policy is governed by [Information Security Steering Group / Risk Committee]. It will be reviewed at least annually, and after any significant incident or organisational change.