|  |
| --- |
| Tips and ideas to foster a positive security culture |

Fostering a positive security culture is crucial for any organisation to effectively manage and mitigate security risks. Here are some tips and ideas that an organisation can implement to cultivate a strong security culture:

**Leadership commitment:** The commitment to security should start from the top management. Leaders should actively promote and communicate the importance of security, set the tone, and lead by example. Regularly reiterate to all staff the importance of cyber security and the potential consequences of security incidents.

**Security awareness training:** Implement regular security awareness training for all staff. Inform your staff about incident reporting procedures, and the organisation's security policies and guidelines. Remember that your staff are both your strongest and weakest link in fighting cyber crime. Help them help your organisation by training them.

**Incentives and recognition:** Recognise and reward employees who demonstrate good security practices or report potential security incidents. This encourages positive behaviour and reinforces the importance of security.

**No blame organisation:** Encourage your staff to be open and transparent when things go wrong. Ensure staff feel comfortable reporting suspicious activities or potential security incidents without fear of getting into trouble.

**Clear policies and procedures:** Develop and communicate clear security policies and procedures that outline the expected behaviours and responsibilities. Encourage employees to ask questions and provide feedback on security practices or concerns.

**Incident response:** Promptly and transparently address reported issues to reinforce the importance of security. Always inform the person who reported the issue about the outcome, and where possible communicate more widely to reinforce the message.

**Secure by design:** Incorporate security considerations into all aspects of the organisation, including product development, system design and business processes. Promote the concept of "secure by design" to ensure security is built-in from the ground up.

**Risk assessments:** Conduct regular risk assessments to identify potential security vulnerabilities and prioritise mitigation efforts based on the level of risk.

**Continuous improvement:** Continuously evaluate and improve the security programme based on feedback, incidents and changing threats. Encourage employees to ask questions, raise concerns, and provide suggestions and ideas for enhancing security.

**Security champions:** Identify and empower security champions within each department or team. They can advocate for security and help promote best practices within their respective groups.

**Collaborative approach:** Foster a collaborative approach to security by involving employees from various departments and levels in the development and implementation of security initiatives.

**Security metrics and reporting:** Establish metrics to measure the effectiveness of the security programme, and regularly report on security performance to stakeholders and employees.

**Third-party assessments:** Consider engaging third-party security experts to conduct independent assessments and audits to identify areas for improvement and validate the effectiveness of the security measures in place (eg, a cyber security maturity assessment to measure your current maturity versus your target maturity).

**Events:** Use messaging and events from other organisations to reinforce your messaging. For example, New Zealand has an annual cyber security smart week in October run by CERT NZ. Use this week to help raise awareness in your organisation. If you sign up to CERT NZ’s Cyber Smart Week, you will receive a range of “ready to use” materials: [Become a 2024 Cyber Smart Week Supporter – confirmsubscription.com](https://confirmsubscription.com/h/d/D7E0E29517B92C0D)

Here are some more tips and ideas you can use to help drive your cyber security journey.

### More tips and ideas

Keep up to date with the work the National Cyber Security Centre (NCSC) are doing to protect New Zealand’s wellbeing and prosperity through trusted cyber security services: [National Cyber Security Centre](https://www.ncsc.govt.nz/)

If you want support with an incident, you can complete an NCSC [Cyber Security Incident Request for Assistance Form](file:///C%3A/Users/lkun/AppData/Local/Microsoft/Windows/INetCache/Content.Outlook/I26YJKUS/NCSC-Incident-Request-for-Assistance-Form.pdf). Or call them on (04) 498 7654 if it is urgent.

CERT NZ have a vast range of security tips and news: [Business – CERT NZ](https://www.cert.govt.nz/business/)

With the increase of cyber crime it is worthwhile having a cyber partner on speed dial in the event you need help.

Formalise cyber security roles and responsibilities in your organisation. Include privacy if your organisation is small or short of resources.

If you are short of time/resources and you have a list of things to do to lift your maturity, do one thing; just don’t do nothing.

Use the material that is available on the Tertiary Education Commission website: [Improving cyber security in the tertiary sector – Tertiary Education Commission](https://www.tec.govt.nz/teo/working-with-teos/improving-cyber-security-in-the-tertiary-sector/)

Understand your risk appetite, agree on this with your organisation and let your staff know.

Keep it simple. Don’t let your desire to be perfect get in the way of being good.

Be patient with your progress; it is a long game.

Utilise your Phriendly Phishing e-learning membership.

Set some budget aside to drive your cyber security work.

It is often more effective to use a third-party provider than try and build your own capability. Leverage managed services.

By implementing these tips and ideas, an organisation can create a culture where security is valued, understood and practised by all employees, reducing the risk of security breaches and protecting the organisation's assets and reputation. You can also use these tips to help drive your organisation’s overall cyber security journey.