Insider threat attacks: security checklist

□ **Monitor departing employees**

- □ Revoke access to systems and data immediately upon departure
- □ Ensure all company devices and sensitive information are returned
- □ Conduct exit interviews to identify any potential risks

□ **Watch for malicious employees**

- □ Monitor unusual behaviour, such as accessing sensitive data
- □ Implement data monitoring tools to track suspicious activity
- □ Limit access to critical data based on role and responsibilities

□ **Address negligent employee actions**

- □ Provide regular cybersecurity training to all employees
- □ Educate staff on the importance of secure data handling
- □ Use role-based access to minimise potential for accidental breaches

□ **Prevent security evasion**

- □ Enforce strict security policies, including strong passwords and MFA
- □ Discourage the use of personal devices for work
- □ Regularly audit employees for compliance with security rules

□ **Limit inside agents' opportunities**

- □ Adopt a zero-trust security model to monitor and restrict access
- □ Continuously vet employees and contractors
- □ se behavioural monitoring tools to detect unusual data transfers

□ **Review third-party access**

- □ Regularly audit third-party access. Restrict it to necessary systems
- □ Ensure vendors follow your security standards
- □ Immediately revoke access when contracts end or roles change