

**Supplier Self Assessment**

**Cyber Security**

1. Does your organisation have a relevant cyber security certification (e.g. ISO 27001)?
2. Does your organisation have a formal cyber security policy?
3. Are the organisation's security policies and procedures reviewed and updated at least annually?
4. When were they last updated?
5. Please briefly describe which areas are addressed within your cyber security policy
6. Does your organisation have established procedures and technical, operational and organisational measures to secure your organisation's cyber security by avoiding disruptions and minimising the impact of security incidents?
7. Has your organisation gone through cyber security audits, assessments and inspections?
8. Does your organisation have a responsible person or team for cyber security within your organisation?
9. Does your organisation use security softwares to protect your systems?
10. Are your systems and software updated regularly?
11. How often are your systems and software updated?
12. Does your organisation enforce access controls and permissions to ensure the protection of sensitive data?
13. Does your organisation have a backup and recovery plan in place?
14. Are employees regularly trained regarding cyber security?
15. How often are employees trained?
16. Does your organisation regularly conduct penetration tests to identify possible security vulnerabilities and to check security measures?
17. Does your organisation have an incident response plan in place for handling cyber security incidents?
18. Does your organisation have a plan for reporting an incident to relevant authorities and how to do so?
19. Has your organisation experienced a cybersecurity incident in the past 12 months?
20. Does your organisation have a process to learn and improve from experienced cyber security incidents?
21. Does your organisation manufacture, distribute or import products with digital elements (e.g., IoT products)?
22. Does your organisation design, develop and manufacture the products with digital elements to ensure an appropriate level of cyber security?
23. Does your organisation or your suppliers offer cyber security updates for the products with digital elements?
24. Does your organisation have a plan for reporting vulnerabilities within or cyber security incidents concerning the products with digital elements?