# OSC Project Cyber Gate Assessment #1

Please complete this checklist and return it by _____. Thank you for your cooperation in ensuring a secure and reliable partnership.

## Company Information

Project Number: Contact Person:
Company Name: Contact Email:

## General Information

1. Does your company have a dedicated IT/security team or person?

☐Yes
☐No
Details:

2. Do you have a documented cybersecurity policy?

☐Yes
☐No
Details:

## Access Control

3. Do you enforce a strong password policy that includes minimum length, complexity requirements, regular password changes, and account lockout after multiple failed login attempts?

☐Yes
☐No
Details:

4. Is multi-factor authentication (MFA) used for access to systems and data?

☐Yes
☐No
Details:

5. Are access rights reviewed and updated regularly? If yes, how regularly?

☐Yes
☐No
Details:

## Data Protection

6. Is data encryption used for information both at rest and in transit?

☐Yes
☐No
Details:

7. Do you have a regular data backup process?

☐Yes
☐No
Details:

8. Are backups tested periodically to ensure data can be restored?

☐Yes

☐No

Details:

### Network Security

9. Do you have security measures in place to protect your company network both in the office and when employees are working remotely, including secure Wi-Fi, VPN usage, and endpoint protection?

☐Yes

☐No

Details:

10. Are security updates and patches applied promptly to all systems?

☐Yes

☐No

Details:

11. Are antivirus and anti-malware solutions installed and updated regularly?

☐Yes

☐No

Details:

### Cloud Security

12. Is data stored in the cloud encrypted?

☐Yes

☐No

Details:

13. Are your cloud services configured according to current security best practices?

☐Yes

☐No

Details:

14. Do you have an incident response plan for cloud-based data breaches?

☐Yes

☐No

Details:

### Monitoring and Compliance

15. Do you have continuous monitoring for your IT systems and networks to detect and respond to cybersecurity threats?

☐Yes

☐No

Details:

16.Are regular vulnerability scans and assessments conducted on your network and systems?
☐Yes
☐No
Details:

### AI Product Security

17.Do you have measures in place to protect AI models and datasets from unauthorized access?
☐Yes
☐No
Details:

18.Do you regularly review and update AI models to address potential vulnerabilities?
☐Yes
☐No
Details:

19.Is there a process in place to monitor AI model performance?
☐Yes
☐No
Details:

### Incident Response

20.Do you have incident detection and response procedures in place that are regularly tested and updated?
☐Yes
☐No
Details:

21.Is there a procedure to document and analyze incidents post-mortem?
☐Yes
☐No
Details:

### Employee Training

22.Do employees receive regular cybersecurity training?
☐Yes
☐No
Details:

23. Are employees trained on the importance of monitoring and reporting suspicious activities?
☐Yes
☐No
Details:

24.Are phishing simulation tests conducted periodically?
☐Yes
☐No
Details:

25.Are new hires provided with cybersecurity training as part of their onboarding process?
☐Yes
☐No
Details:

## Compliance and Review

26.Is there a schedule for reviewing and updating cybersecurity policies?
☐Yes
☐No
Details:

27.Do you ensure regulatory compliance (e.g., GDPR, EU AI Act) in your cybersecurity efforts?
☐Yes
☐No
Details:

28.Are cybersecurity policies communicated and enforced within your organization?
☐Yes
☐No
Details:

29.Do you have a process for identifying and mitigating third-party risks?
☐Yes
☐No
Details:

## Additional Comments:

30.Please provide any additional information or context that may be relevant to your cybersecurity practices.
Details:

## Attestation of Project Participant:

On behalf of _____ , I hereby declare that the above information is complete and accurate.
Name:
Authorized Signature:

Date: