

Appendix - Supplier Self-Assessment on information security

1. Organizational Security

Is there a certified information security management system?

☐ ISO 27001

☐ TISAX

☐ No

Remark:

Has a person responsible for information security been appointed and is this person known to all staff?

☐ Yes / ☐ No

Is there an information security management system (ISMS) that includes at least the following components?

- Description of the ISMS
- Information Security Policies
- Information Security Risk Management Process
- Continuous improvement

☐ Yes / ☐ No

Is there an implemented concept for the management and protection of mobile devices (smartphones, tablets, laptops, storage media)?

☐ Yes / ☐ No

Remark:

Is there an implemented approach to access and protection to cloud services?

☐ Yes / ☐ No

Are regular awareness trainings of the entire staff carried out?

☐ Yes / ☐ No

Does your company have cyber insurance?

☐ Yes / ☐ No

2. Operational Security

Does your company develop software or software components for BING?

☐ Yes / ☐ No

Is there an implemented concept for data backup and are backups regularly checked?

☐ Yes / ☐ No

Remark:

Is business continuity management and corresponding contingency plans in place?

☐ Yes / ☐ No

Are there effective measures to protect against scams and phishing emails?

☐ Yes / ☐ No

Are all remote and cloud access secured with multi-factor authentication?

☐ Yes / ☐ No

Is there centrally managed protection against malware?

☐ Yes / ☐ No

Is there a centrally managed EDR/XDR system?

☐ Yes / ☐ No

Is there an implemented patch management approach that covers operating systems and application software?

☐ Yes / ☐ No

Is there an implemented concept for log management?

☐ Yes / ☐ No

Confirmation

I hereby confirm that the information on this form is complete and correct:

Name _____

Department / Position: _____

Place, Date / Signature _____