### The purpose of this checklist is to evaluate our Supplier’s cybersecurity management by covering key topics that help limit the risk and impact of a cybersecurity attack. Information shared by Infineum with current or potential Suppliers must be kept secure. Return completed checklist to your Infineum contact as requested.

1. Do you have any policies in place relating to data privacy and protection, as well as cybersecurity? Choose an item.

2. Are your policies checked, updated on a regular basis, and enforced? Choose an item.

3. Do you subscribe to cybersecurity updates so that you are aware of threats? Choose an item.

4. Do you have an effective cybersecurity incident response plan, and do you test and update it regularly? Choose an item.

5. Does your company have written business continuity/disaster recovery plans, and do you test and update it regularly? Choose an item.

6. What certifications does your company (and any external IT solutions provider) have (eg. ISO 27001 (managing information security), SOC, etc.) and can you provide documentation? Click or tap here to enter text.

7. Does your company have a process for training and testing employees on cybersecurity best practices? Choose an item.

8. Do you have an effective data backup solution, and do you perform restore tests regularly? Choose an item.

9. Does your company have written controls plan that contains the administrative, technical and physical safeguards you use to collect, process, protect, store, transmit, dispose or otherwise handle our data (e.g., Information Security Plan)? Choose an item.

10. Have you classified data by privacy, sensitivity and risk? Choose an item.

11. Does your company maintain up-to-date versions of anti-virus software, anti-malware, antispyware, and operating systems security patches? Please elaborate. Click or tap here to enter text.

12. Does your company ensure adequate steps are taken to guard against unauthorized access to our company data (e.g., firewall)? Please list the technology and processes that are in place. Click or tap here to enter text.

13. Do you conduct periodic checks that your controls are operating properly, such as vulnerability assessment and penetration tests? Choose an item.

14. Do you assess third parties for cybersecurity risk? Choose an item.

15. Do you build appropriate contractual obligations on third parties to mitigate cybersecurity threats? Choose an item.

Any additional comments? Click or tap here to enter text.