Security operations centre (SOC)

Service Level Agreement (SLA)

xentra

Building technology infrastructures unique to your needs

0113 526 3475
support@xentra.co.uk
xentra.co.uk

Service Level Agreement (SLA)

We understand that time is of the essence when dealing with cybersecurity incidents. That's why we establish clear, actionable SLAs for each incident classification to guarantee that your security needs are met within defined timeframes. Our SLA framework includes:

- Response Time: The time it takes to acknowledge and begin addressing an incident after detection. Critical incidents are prioritised with the fastest response times to minimise risk to your organisation.

- Resolution Time: The time within which an incident is expected to be fully resolved. For example, critical incidents may be resolved within hours, while lower-priority incidents are handled according to agreed-upon timelines.

By defining these SLA targets upfront, we provide full transparency and accountability, ensuring that our SOC team addresses incidents promptly and minimises organisation disruption. We are committed to meeting these service levels consistently, which results in faster threat mitigation, less downtime, and a more resilient security posture for your organisation.

With our Incident Classification and SLA framework in place, your organisation can rest assured that cybersecurity incidents will be prioritised, managed, and resolved in line with both best practices and your unique organisation requirements. We strive to offer proactive, timely, and effective cybersecurity operations that allow you to focus on your core organisation objectives, knowing your digital assets are protected.

Service Level Agreement (SLA)

Incident response and classification:

Priority Level	Description	Response Time	Method of Contact	Xentra CSIRT Response
P1 Critical	Immediate action necessary to mitigate current malicious activity	1 hour	Call/email **Included in end of month report*	Investigation
P2 High	High potential for incident if preventive action is not taken	1 hour	Email **Included in end of month report*	Investigation
P3 Medium	Low potential for incident	4 hours	Email **Included in end of month report*	Incident checked & resolved
P4 Low	Very low potential for incident/ informational or maintenance type activities	24 hours	Email **Included in end of month report*	Incident checked & resolved

If you have any questions, please do not hesitate to get in touch with your dedicated account manager or our support team.

xentra

Building technology infrastructures unique to your needs

0113 526 3475
support@xentra.co.uk
xentra.co.uk