ANNEXURE-III

SCOPE OF WORK

1. **XDR (Extended Detection and Response) Services** for end-user systems.
2. **MDR (Managed Detection and Response) Services** for servers.

Scope of Work:

For XDR Services (End-User Systems):

- Deployment of XDR solution across all end-user devices (desktops, laptops, etc.).
- Centralized threat detection and response against malware, ransomware, phishing, and advanced persistent threats (APTs).
- Continuous monitoring with automated incident detection and response.
- Policy-based security controls and endpoint protection.
- Regular updates, patch management assistance, and system hardening recommendations.
- Monthly/quarterly security posture and threat activity reports.

For MDR Services (Servers):

- 24x7 monitoring of critical institutional servers (on-premises and/or cloud-based).
- Threat hunting, analysis, and real-time incident response.
- Log collection, correlation, and analysis from servers.
- Immediate escalation and remediation support for detected threats.
- Compliance-focused monitoring (HIPAA, ISO, PCI-DSS, etc. as applicable).
- Periodic vulnerability assessments and server health reports.

General Deliverables:

- Integration of XDR & MDR solutions with existing IT infrastructure (firewalls, SIEM, etc.).
- Knowledge transfer and training sessions for internal IT staff.
- Dedicated support team with escalation matrix.
- Service Level Agreement (SLA) defining response and resolution timelines.