CYBER SECURITY

DAY 1: CYBER SECURITY FOUNDATIONS AND THREAT LANDSCAPE

Session	Time	Session Topic	Detailed Content
1	10:00 AM - 11:15 AM	**Cyber Security Context for Digital and Operational Systems**	• Role of cyber security in maintaining confidentiality, integrity, availability, safety and continuity of operations. • Coverage of IT systems, OT/SCADA environments, endpoints, networks, communication systems, applications and data. • Shared responsibilities of users, IT teams, OT teams, management, vendors and service providers.
2	11:30 AM - 12:45 PM	**Threat Actors, Attack Paths and Common Incidents**	• Phishing, malware, ransomware, credential theft, social engineering, unauthorised access and supply-chain compromise. • Typical attack paths through email, remote access, removable media, internet exposure, weak credentials and third parties. • Operational and organisational impact including data loss, service disruption, unsafe conditions and reputational/audit consequences.
3	2:30 PM - 3:45 PM	**IT, OT and SCADA Security Differences**	• Differences in objectives, architecture, lifecycle, availability requirements and change management between IT and OT. • Risks related to legacy systems, vendor access, protocol exposure, engineering workstations and weak network separation. • Need for coordinated controls that protect operations without unsafe or unapproved changes.
4	4:15 PM - 6:00 PM	**Applicable Cyber Governance and Reporting Framework**	• Overview of organisational cyber policy, applicable statutory/sectoral requirements and roles of designated cyber authorities. • Asset ownership, risk accountability, authorised access, incident reporting and evidence preservation. • Need to follow current advisories, approved SOPs and escalation channels rather than informal response.

CYBER SECURITY

DAY 2: IDENTITY, ACCESS, NETWORK AND ENDPOINT SECURITY

Session	Time	Session Topic	Detailed Content
1	10:00 AM - 11:15 AM	**Identity and Access Management**	• User identity, role-based access, least privilege, need-to-know and segregation of duties. • Account creation, modification, review, suspension and deactivation; risks of shared and dormant accounts. • Privileged access, vendor access, approval controls, logging and periodic recertification.
2	11:30 AM - 12:45 PM	**Passwords, Multi-Factor Authentication and Credential Safety**	• Strong password/passphrase practices, password managers where approved and avoidance of password reuse or sharing. • Use of multi-factor authentication, login alerts, lockout controls and secure recovery processes. • Recognition and reporting of suspected credential compromise.
3	2:30 PM - 3:45 PM	**Network Segmentation, Remote Access and Secure Connectivity**	• Basic network zones, segmentation, controlled gateways and separation of business and operational systems. • Secure remote access, VPN, jump hosts, vendor sessions, approval windows and session monitoring. • Risks of public Wi-Fi, unauthorised hotspots, open ports, unknown devices and unapproved remote tools.
4	4:15 PM - 6:00 PM	**Endpoint, Patch and Removable-Media Security**	• Security controls for desktops, laptops, servers, engineering workstations and mobile devices. • Patch/vulnerability management, approved software, anti-malware, configuration control and exception handling. • Controlled use and scanning of USB/removable media; reporting abnormal system behaviour.

CYBER SECURITY

DAY 3: EMAIL, DATA, BACKUP AND THIRD-PARTY SECURITY

Session	Time	Session Topic	Detailed Content
1	10:00 AM - 11:15 AM	**Phishing and Social Engineering Defence**	• Identification of suspicious senders, domains, links, attachments, urgent requests and impersonation attempts. • Verification of payment, password-reset, access and information requests through approved channels. • Safe response: do not click, do not forward internally, report promptly and preserve evidence.
2	11:30 AM - 12:45 PM	**Data Classification, Protection and Secure Sharing**	• Identification and handling of public, internal, confidential, personal and operationally sensitive information. • Need-to-know access, encryption where approved, controlled file sharing, secure disposal and prevention of unnecessary copying. • Safe handling of screenshots, drawings, system details, employee/participant data and credentials.
3	2:30 PM - 3:45 PM	**Backup, Recovery and Ransomware Resilience**	• Backup scope, frequency, offline/segregated copies, retention, restoration testing and ownership. • User and system responsibilities during data loss, corruption, ransomware suspicion or storage failure. • Recovery prioritisation, evidence preservation and controlled restoration under authorised technical guidance.
4	4:15 PM - 6:00 PM	**Vendor, Supply-Chain and Cloud Security**	• Cyber requirements in procurement, onboarding, remote support, software/firmware updates and service contracts. • Due diligence, access limitation, logging, data-location considerations, incident notification and exit controls. • Risks of unverified tools, default credentials, unsupported software and uncontrolled third-party data sharing.

CYBER SECURITY

DAY 4: MONITORING, INCIDENT RESPONSE AND OT CONTINUITY

Session	Time	Session Topic	Detailed Content
1	10:00 AM - 11:15 AM	**Cyber Event Detection and Initial Triage**	• Indicators such as unusual login alerts, unknown files, abnormal traffic, unexpected configuration changes and suspicious emails. • Distinguishing routine faults from potential cyber events while avoiding unauthorised investigation or changes. • Capturing time, system, user action, screenshots, alerts and other initial evidence.
2	11:30 AM - 12:45 PM	**Incident Reporting and Escalation**	• What to report, when to report, whom to contact and information required in an initial incident report. • Timely escalation, preservation of logs/evidence, confidentiality and communication control. • Documentation of decisions, containment actions, recovery status and closure.
3	2:30 PM - 3:45 PM	**Containment, Recovery and Business / Operational Continuity**	• Authorised containment principles including isolation, access restriction, blocking and preservation of affected systems. • Coordination among cyber, IT, OT, operations, safety, communication, legal and management functions. • Restoration priorities, validation, monitoring and lessons learned after recovery.
4	4:15 PM - 6:00 PM	**Practical Cyber Incident Tabletop Exercise**	• Scenario involving phishing-led credential compromise with possible movement toward operational systems. • Group preparation of detection, reporting, escalation, containment, continuity and evidence-preservation actions. • Facilitated review of control gaps, role clarity and decision points.

CYBER SECURITY

DAY 5: RISK ASSESSMENT, CYBER HYGIENE AND APPLICATION

Session	Time	Session Topic	Detailed Content
1	10:00 AM - 11:15 AM	**Cyber Risk Assessment and Control Prioritisation**	• Identification of assets, threats, vulnerabilities, existing controls, impact and risk ownership. • Risk treatment options: reduce, avoid, transfer or accept through authorised governance. • Prioritisation based on operational criticality, exploitability, exposure and consequence.
2	11:30 AM - 12:45 PM	**Daily Cyber Hygiene and Secure Work Practices**	• Screen lock, software updates, secure email, approved devices, safe browsing, password discipline and clean-desk practices. • Secure practices for travel, remote work, online meetings, mobile communication and information sharing. • Practical departmental checklist for routine compliance and supervisory review.
3	2:30 PM - 3:45 PM	**Department-Level Cyber Risk Exercise**	• Group identification of cyber risks in IT, OT, SCADA, projects, procurement, finance, administration and field workflows. • Mapping preventive, detective, reporting, recovery and documentation controls for selected risks. • Review of ownership, feasibility, dependencies and escalation requirements.
4	4:15 PM - 6:00 PM	**Group Presentation, Review and Action Plan**	• Presentation and review of departmental cyber-risk controls and incident-response actions. • Consolidated recap of identity, network, endpoint, data, backup, vendor, incident and OT-security requirements. • Post-assessment and preparation of practical cyber-hygiene and risk-reduction action points.