| Role Profile – The What, The Where, The How | | | |
|---|---|---|---|
| POSITION | Cyber and Endpoint Security Engineer | | |
| TEAM | ICT | LOCATION | Coastline House |
| VERSION | 2.0 | LAST UPDATED | October 2026 |

| | |
|---|---|
| THE PURPOSE OF THIS ROLE IS TO | Be responsible for protecting Coastline's information assets, identities, infrastructure, cloud services and endpoint devices through proactive monitoring, threat detection, vulnerability management, security engineering and continuous improvement of cyber security controls.<br><br>The role combines hands-on cyber security expertise with endpoint security and management, identity and access security, vulnerability remediation, patch governance, platform maintenance and security assurance. Working closely with the Networking and Infrastructure team, the post holder will help ensure Coastline's technology services are securely configured, appropriately maintained, resilient and aligned with recognised industry frameworks and organisational risk priorities.<br><br>The Cyber and Endpoint Security Engineer serves as Coastline's principal technical cyber security specialist and provides expert guidance, assurance and technical leadership across cyber security, endpoint management, identity management and infrastructure security disciplines. You will work closely with the Governance team to support the development of clear, practical policies including safe and responsible use of AI by end users. You will provide specialist technical security advice and configure and implement the technical policies and controls that put these requirements into practice.<br>The role will support the development, implementation and continuous improvement of security controls aligned with the NIST Cybersecurity Framework (CSF) 2.0, CIS Controls, Cyber Essentials Plus, ISO/IEC 27001 and other recognised security standards and good practice. |

## Specific Accountabilities – The Brass Tacks

In the role, day to day, you'll be responsible for:

### Security Monitoring and Incident Response

1. Monitor, triage and investigate security alerts across SIEM, EDR, cloud, network, identity and endpoint security platforms; identify, analyse and escalate potential incidents, indicators of compromise and suspicious activity; and research emerging threats, attack techniques, vulnerabilities and cyber security trends.

2. Support and coordinate cyber incident response in accordance with agreed plans and escalation arrangements, including investigation, containment, eradication, recovery and lessons learned; participate in post-incident reviews and implement agreed improvements.
3. Act as the primary technical liaison with Coastline's MSSP, SOC and other specialist security providers; review security service performance and manage escalated cyber security investigations.

### Vulnerability Management, Patching and Maintenance

4. Conduct vulnerability assessments across infrastructure, applications, cloud services, network devices, identities and endpoints; assess, prioritise and track remediation based on risk, exploitability, business impact and organisational priorities; and validate remediation through verification scanning, testing and security assurance reviews.
5. Lead the technical coordination and assurance of vulnerability remediation, security patching, firmware updates and critical fixes; provide recommendations and reporting to the IT Manager; agree delivery responsibilities with Infrastructure, Networking and other service owners; and plan, test, implement and validate security updates and platform maintenance.
6. Monitor patch compliance, remediation effectiveness and security-update deployment success; coordinate emergency remediation for actively exploited vulnerabilities and critical advisories; and produce vulnerability, threat, patching, remediation, risk and exposure-management reporting for management, the executive team and the board.
7. Support platform lifecycle management, technology refreshes, certificate renewals, system upgrades and end-of-life remediation activities.

### Endpoint Engineering and Endpoint Security

8. Design, implement, support and continually improve endpoint security controls across all supported device platforms; administer associated security technologies; and coordinate changes to endpoint management controls with colleagues responsible for device configuration and user experience.
9. Develop and maintain endpoint compliance and device-control policies, security baselines, application-protection standards and attack-surface-reduction controls; support secure device provisioning, deployment, configuration and lifecycle management; and maintain endpoint hardening standards and secure configuration baselines, with deviations and exceptions documented and reviewed.
10. Monitor endpoint security posture and remediate non-compliant, vulnerable or unsupported devices; evaluate new endpoint management and security technologies that improve resilience and efficiency; and support endpoint automation and continual service improvement.

### Identity and Access Security

11. Design, implement and continually improve security controls within Microsoft Entra ID and associated identity platforms; administer Conditional Access, MFA, Privileged Identity Management, Identity Protection and Zero Trust controls; and assist with secure integration of on-premises and cloud identity services.
12. Monitor and investigate identity risks, sign-in anomalies and privileged-access activity; review privileged and service accounts, administrative roles and permissions for least

privilege; and support identity governance, access reviews, joiner-mover-leaver processes and privileged-access management.

13. Work with system owners to maintain secure authentication, authorisation and access management, and maintain identity-security documentation, standards and operational procedures.

### Infrastructure and Network Security Collaboration

14. Assist the Networking and Infrastructure team to design, implement, maintain and improve secure infrastructure and network services; provide specialist cyber security expertise and assurance to the IT Manager, Service Desk, infrastructure & networking teams; and support secure network, server and cloud-platform configurations.
15. Review infrastructure and network changes to ensure appropriate security controls, testing and rollback arrangements; support secure network, server and cloud-platform configurations; review environments against agreed baselines, hardening standards and industry good practice; and collaborate on business continuity, disaster recovery and resilience where they affect cyber security posture.
16. Support network-security controls, logging, monitoring, segmentation and secure remote access; and contribute to security architecture reviews, technical standards and technology-selection decisions.

### AI Security, Acceptable Use and Governance

17. Work with Governance to develop, implement, maintain and improve policies for safe and responsible end-user AI use; provide specialist advice and implement supporting technical policies, standards and controls; and explain the security implications of conversational AI and AI agents, including connected data, applications, tools, workflows and agent capabilities.
18. Set proportionate technical security requirements for AI services based on permissions, persistent context, organisational data access and ability to execute actions; and define acceptable-use requirements with Governance covering approved services and accounts, permitted inputs, access controls, data handling, retention, sharing, human oversight and prohibited uses.
19. Assess security, identity, permission and data-access risks for proposed AI services, agents, connectors, integrations and plugins before implementation or wider adoption; work with information governance, data protection, business owners and the IT Manager to translate governance requirements into enforceable controls and operational guidance.
20. Monitor approved AI capabilities where suitable tooling exists, identify misuse or excessive access and recommend corrective controls; maintain review processes for exceptions and emerging capabilities; and provide practical guidance and awareness material on the differing risks and responsibilities of AI chat and AI agents.

### Security Governance, Frameworks and Continuous Improvement

21. Develop and improve controls aligned with NIST CSF 2.0, CIS Controls, Cyber Essentials Plus and ISO/IEC 27001; perform control assessments, gap analyses and maturity reviews; and support governance, risk management, compliance and audit activities.
22. Develop and maintain technical security standards, hardening baselines, procedures and operational documentation; identify security risks and recommend practical treatment and

remediation; and produce cyber security dashboards, KPIs, metrics, management reports and assurance information.

23. Support successful internal and external audits, assessments and accreditations; evaluate emerging security technologies, automate security processes where appropriate and identify opportunities to improve cyber security maturity.
24. Contribute to Coastline's cyber security strategy and roadmap under the direction of the IT Manager.

| Person Specification – The Who | |
|---|---|
| PERSONAL SKILLS AND QUALITIES | At Coastline we are more concerned with how you work and what you bring to the role over formal qualifications or criteria. Specifically, what we're looking for is someone who:<br>• Demonstrates behaviours in accordance with Coastline's values:<br>  ○ Put our customers first<br>  ○ Be open, honest and accountable<br>  ○ Value each other<br>  ○ Strive to be the best<br>• Degree or equivalent experience in Cyber Security, Endpoint Management and relevant IT qualification(s).<br>• Completes a satisfactory Enhanced DBS check.<br>**Essential Experience and Knowledge**<br>• Experience working within cyber security operations, security engineering, threat monitoring and incident response environments, including practical knowledge of SIEM, EDR, vulnerability management and security monitoring tools.<br>• Strong practical experience of endpoint management and endpoint security across modern enterprise environments.<br>• Experience administering the Microsoft Security Eco System in a production environment.<br>• Experience implementing and managing Conditional Access, MFA, Identity Protection and Privileged Identity Management solutions, with knowledge of Zero Trust principles.<br>• Strong knowledge of vulnerability management, patch deployment, firmware updates, remediation tracking and security assurance practices. |

- Experience maintaining secure configuration baselines and system-hardening standards across endpoints, servers and cloud services.
- Experience supporting the security of Windows Server, cloud services, endpoint platforms and network infrastructure, including collaboration with the teams responsible for their day-to-day operation.
- Good understanding of networking principles and infrastructure security, including segmentation, firewalls, remote access, secure administration, logging and monitoring.
- Experience supporting technology lifecycle activities, including platform upgrades, certificate renewals, maintenance, decommissioning and end-of-life remediation.
- Experience producing and collating security reports, dashboards, metrics and management information.
- Strong analytical, investigative, problem-solving and troubleshooting abilities.
- Ability to assess technical risk, prioritise remediation and communicate residual risk to technical and non-technical stakeholders.
- Experience collaborating with infrastructure, network, service delivery and project teams.
- Strong verbal and written communication, stakeholder and supplier management, and organisational skills, including the ability to manage multiple priorities.
- Ability to work with governance colleagues to develop clear policies and guidance for emerging technologies, translate agreed requirements into technical configurations and controls, and explain the security implications of end-user AI, AI agents, connected tools, permissions and organisational data access.

### Frameworks and Governance Knowledge

- Sound working knowledge of the NIST Cybersecurity Framework (CSF) 2.0 and its practical application.
- Understanding of Cyber Essentials Plus requirements and assessment expectations.
- Understanding of CIS Controls and their practical implementation.
- Understanding of ISO/IEC 27001 security principles and control frameworks.
- Ability to translate security framework and organisational policy requirements into practical technical controls, prioritised remediation plans and operational improvements.

| | |
|---|---|
| | Some experience in the following would be an advantage:<br>• Relevant cyber security certification such as Security+, Microsoft Security, SC-200, SC-300, MD-102, AZ-500, CISSP, CISM, CRISC or equivalent, or willingness to achieve one.<br>• Experience with SIEM platforms.<br>• Experience with Microsoft Defender Vulnerability Management or an equivalent vulnerability-management platform.<br>• Experience supporting Cyber Essentials Plus, ISO/IEC 27001 or formal security audits.<br>• Knowledge of PowerShell, Microsoft Graph or other scripting and security-automation technologies.<br>• Knowledge of Windows Server, Active Directory, Group Policy, Microsoft Azure and hybrid identity environments.<br>• Experience implementing security controls or governance for enterprise AI services, including AI assistants, chat experiences, agentic systems or workflow-integrated AI.<br>• Ability to travel between Coastline sites when required.<br>• Willingness to participate in cyber incident response and occasional out-of-hours support. |

| General Obligations - For All Of Us |
|---|
| 1. Represent the company positively with all external agencies.<br>2. Service and support the company as requested.<br>3. Establish, develop and maintain effective working relationships with all work colleagues.<br>4. Ensure compliance with the company's health and safety policies and procedures.<br>5. Continually promote equal opportunities and customer care in full compliance with the company's policy and standards. |

| REPORTING |
|---|
| The Cyber and Endpoint Security Engineer is Coastline's lead technical cyber security specialist and reports directly to the IT Manager.<br>The role is responsible for the implementation, operation and continual improvement of technical security controls across endpoint, identity, infrastructure and cloud platforms.<br>The role works closely with the Service Desk, Infrastructure and Networking teams, providing security expertise, technical assurance and specialist guidance while supporting the IT Manager in delivering Coastline's cyber security strategy, framework obligations, compliance objectives and secure adoption of AI capabilities. |

The role leads the technical delivery, assurance, monitoring and coordination of endpoint, identity, patching, infrastructure and end-user AI security controls. Overall service ownership, prioritisation, policy approval and risk acceptance follow Coastline's agreed governance and delegated-authority arrangements, with the role providing technical advice to the IT Manager, Governance team and relevant service owners. Operational ownership of core network and infrastructure services remains with the relevant technical teams, with shared responsibility for implementing and maintaining agreed security controls.

## CONTACTS

### Internal

- All staff
- ICT Team
- Governance Team
- Leadership Team
- Project teams and business stakeholders

### External

- IT suppliers and technology partners
- Managed Security Service Providers (MSSPs) and Security Operations Centre providers
- Auditors, assessors, consultants and contractors
- Customers, customer representatives, housing associations, local authorities, housing corporations and other government bodies
- Regulatory and industry bodies where required