## Bernicia Group Role Profile

**Title**:  Cyber Analyst

**Reporting to**:  Head of Security and Infrastructure

**Date**: January, 2026

## Purpose

Assist the Head of Security and Infrastructure in protecting Bernicia's computer networks and systems from cyber threats by monitoring, analysing and responding to security incidents.

## Accountabilities

### Operational

1. Maintain and monitor the groups Cyber Security product portfolio to identify security improvements and investigate and prevent system intrusion or compromise.
2. Continuously observe network activity for signs of unauthorised access or anomalies.
3. Conduct regular vulnerability assessments of systems and networks to identify potential vulnerabilities and recommend remediation strategies.
4. Create and promote best practices for information security within the organisation.
5. Regularly review the cyber training in place to ensure it remains current, and identify and implement improvements.
6. Perform periodic risk assessments and penetration tests to evaluate the effectiveness of security measures.
7. Investigate security breaches and respond to incidents in real-time, documenting findings and actions taken.
8. Provide support to and cover for the Head of Security and Infrastructure.
9. Provide support for the Director, ICT for the procurement of cyber-related systems.

10. Monitor internal cyber security-related changes to ensure the change and the processes are robust and accurate.
11. Provide technically sound advice and guidance to any department, officers and members on ICT software and hardware issues and to communicate this clearly and unambiguously.

## Strategic

1. Perform research and alert the Head of Security and Infrastructure function to any emerging Cyber Security threats.
2. Stay updated on the latest cyber threats and trends to enhance the organisations security posture.

## Corporate

**Conduct and Other Responsibilities**

1. To display appropriate conduct at all times as a member of staff of the organisation and to observe and promote the code of conduct, health and safety, equality and diversity and customer care policies and all other policies and procedures.

2. To ensure that all Group activities are discharged in a safe manner, minimising risk, at all times.

3. To attend learning and development events, as required.

4. To maximise the use of ICT facilities and contribute to their development where appropriate.

5. To carry out any other duties appropriate to the post, as required or requested by the line manager.

The above list is not exhaustive and your role will certainly change over time reflecting the changing needs and activities of the organisation and our commitment to making best use of new technology and continuously improving the way we do things.  You must therefore be committed to personal development and to becoming multi-skilled in order that you can adapt to and welcome constant change in the effort to achieve the stated aim of “making continuous improvements in the efficiency and effectiveness of our use of resources”.

All staff are encouraged not to ignore work at the boundaries of their specific role, but to take “ownership” of any issue with which they become involved, ensuring that all matters are brought to a satisfactory conclusion.  This includes identifying any risks involved in the day to day responsibilities of the role and taking action to mitigate those risks.

You must carry out your duties with full regard to the Bernicia Way and must draw to their manager's attention any unsafe working practice/conditions.

## Desirable Skills & Experience

**Essential criteria:**
An understanding of modern Security principles and technologies
Al least 1 year's experience and proficiency with cyber security tools and technologies including firewalls, intrusion detection and SIEM systems
Strong analytical and pro-active problem-solving skills
Ability to communicate technical information clearly to non-technical stakeholders and collaborate with other IT professionals.

**Desirable criteria:**
Relevant certification such as CompTIA Security+, Security Blue Team, Certified Ethical Hacker (CEH)
Experience with threat hunting and incident response

Signed by Post holder…………………………………………… Date ……………………

Signed by Manager …………………………………………… Date ……………………

## Values

| Value | Expectation |
|---|---|
| Customer Focussed | Because we care about our customers, how we do things is as important to us as what we do. We understand our customers and deliver great customer service. |
| Teamwork | We work together, across boundaries, to meet the needs of our customers and help the organisation to be successful. |
| Integrity | We uphold the highest standards of integrity in all of our actions. |
| Respect for People | We value our people, encourage their development and reward their performance. |

| | |
|---|---|
| Leadership | We provide strong corporate governance and leadership which is out-come focussed. |
| Accountability | We are personally accountable for delivering on our commitments. |

MINDFUL EMPLOYER

disability confident EMPLOYER

INVESTORS IN PEOPLE | Gold