Job Description

Operated by West Midlands Trains

Information Security Manager

Reports to: Head of Security and Emergency Planning

Grade: PM02

Safety Status: Non-critical

Date version agreed: 13/12/2021

1. Job Purpose

- To be the key driver of the design, delivery and embedding of the information security principles within WMT's IT Security Strategies.
- Working in partnership with Group and company management to identify and evaluate IT and data risks and support the development of effective practical solutions to any issues arising.
- Act as Data Protection Manager, building in data management to IT and business strategies.
- Provide advice and guidance to directors, management and staff at all levels in IT risk, control, compliance and governance issues.

2. Safety Details

A. This job requires **Security Clearance** (e.g. Running of Special Trains) ☐

B. The job holder is required to hold a relevant **Track Safety** competence (e.g. PTS) ☐

C. This is a **Safety Critical Work Post** ☐

D. This is a **Key Safety Post** ☐

E. Reference to this job is included in West Midlands Trains' **Safety Certification** documents ☐

F. This job **Manages Employees** (undertakes specific tasks indicated in the occupational & operational standards manuals) ☐

G. This job **Manages Locations** (undertakes specific tasks as indicated in the occupational and operational standards manuals) ☐

3. Dimensions

A. Financial: None

B. Staff: None

---

4. Principle Accountabilities

- Perform regular reviews of where West Midlands Trains currently sits in regards to ISO 27001 compliance and identify the risks created by non-compliance
- Formulate and maintain an IT and Data Security implementation plan in conjunction with the IT team to provide a professional IT and data security risk assurance service to the business
- Contribute to the design of the policies, procedures and controls required to mitigate IT and data security risks into the wider business
- Develop detailed work plans to assess and report on the business' compliance with all IT Security requirements including, but not limited to, Cyber Essentials, Network and Information Systems (NIS) Directive, National Railways Security Programme (NRSP) and PCI DSS
- Promote the continuous improvement of IT Security Risk Management and control processes by developing a proactive, operational focused relationship with management, ensuring that issues identified are resolved
- Be responsible for the stewardship of electronic assets and data throughout the organisation, including recording, retention and disposal
- Perform WMT's Data Protection Manager responsibilities, working with the Group DPO and the business to improve on data controls
- Manage own workload including planning the scope, aim and objective of each review, with a view to ensuring that key risk areas are assessed and evaluated
- Communicate key issues and solutions to management by producing clear, concise and timely reports, presentations, etc
- Represent WMT at the Abellio UK Group steering groups, assuming responsibility for all outputs from this forum
- Develop and enhance technical, inter-personal and managerial skills and business awareness

---

5. Context

A: Operating Environment:

Provide all levels of management within the business with assurance as to the adequacy and effectiveness of Information Security, risk management, control and corporate governance processes.

The role is required to be familiar with operational structure and responsibilities of each function within the company.

B: Framework and Boundaries:

West Midlands Trains and Abellio UK Group Policies & Procedures Manual impact on the role through compliance with Information Security Policy, Data Protection Policy and related procedures set out within other policies.

C: Organisation:
Report into the Head of Security and Emergency Planning.

---

6. Relationships

A: Reporting lines
Report to Head of Security and Emergency Planning. Periodic one-to-ones are carried out to review progress and performance against objectives. There is likely to be daily contact with Head of Security and Emergency Planning for any operational matters.

B: Other Contacts:
(i) Within the Company:

- Work closely with the West Midlands Trains-based IT team on a day-to-day basis providing policy guidance, advice and support
- West Midlands Trains management and staff at all levels on a frequent basis through interactions whilst carrying out activities pertaining to the role
- Work with the HSSE Directorate on all issues relating to Security both virtual and physical.

(ii) Outside the Company:

- Represent West Midlands Trains on the Abellio UK Group steering groups
- Represent West Midlands Trains on the wider rail focused cybersecurity and data privacy support groups

---

7. Knowledge and Experience

- Experience of implementing ISO 27001 standards in a rapidly changing organisation
- Experience of managing and implementing the NIS(D) for an OES/CNI
- Experience of managing compliance with the Data Protection Act 2018
- Experience of maintaining Information Security policies and processes
- Experience of managing and reporting on PCI DSS
- Understanding of the IEC/62443 Standard
- Excellent analytical skills, together with an attention to detail
- Self-motivated and well organised
- Excellent verbal and written communication skills & ability to deal with individuals at all levels
- CISM/CRISC or CISSP qualifications desirable

---

8. Job Challenge(s):

The role will evolve in three key stages:

- Compliance with functional standards such as ISO 27001, the NIS(D) and PCI DSS and associated cybersecurity risks.
- Management and maintenance of the policies, procedures and controls required to mitigate these risks into the wider business.
- Maintenance of the Training and Awareness programme across all areas of the business.
- Advise and consult when required to protect the business from information risk associated with business as usual or projects by implementing security by design.

The findings should be reported to management with practical and cost-effective recommendations to identified control weaknesses and operational inefficiencies in order to improve the control environment, but additionally to improve the functionality of each area of the business.

9. Additional Information

None

10. Sign off

Job Holder:..... Date:.....

Manager:..... Date:.....

Nominated Deputies

If this is a KEY SAFETY POST (2D is "checked") a Nominated Deputy must be identified. The job holder must ensure that the Nominated Deputy receives a copy of, and is briefed on, this Job Description.

Job title of Nominated Deputy: .....

Name of Nominated Deputy: .....

Signature of Nominated Deputy: .....

Date: .....

As the Nominated Deputy for this post, I confirm that I have been briefed on the requirements of this job. If there are more Nominated Deputies they should sign further copies of this Job Description.