JOB DESCRIPTION

JOB TITLE:	Information Security & Support Analyst
LOCATION:	London
COMPANY:	Resolution Life Group Services
REPORTS TO:	Tbc
GROUP WIDE INTERNAL LEVEL:	Manager

POSITION SUMMARY:

The Information Security and Support Analyst will be accountable for definition, implementation, execution, and achievement of desired outcomes for the Information Security and internal IT support function and posture for Resolution Life Group Services. Primary accountability is to provide IT Security and support to Resolution Life Services team.

KEY ACCOUNTABILITIES:

- Establish a robust Information Security framework for the company that is aligned to the NIST CST and ISO 270001 industry standards.
- Monitor computer networks for security issues.
- Investigate security breaches and other cyber security incidents.
- Document security breaches and assess the damage they cause.
- Work with security team to perform tests and uncover network vulnerabilities.
- Fix detected vulnerabilities to maintain a high-security standard.
- Stay current on IT security trends and news.
- Develop company-wide best practices for IT security.
- Help colleagues install security software and understand information security management.
- Research security enhancements and make recommendations to management.
- Stay up to date on information technology trends and security standards.
- Develop oversight processes for monitoring security threats and response tactics for security breaches.
- Manage and direct the investigation of security incidents related to non-compliance with internal policy standards and external regulations for abuses of company's electronic communication systems.
- Provide direction for the integrity of the company’s Information Systems by developing standards and safeguards that protect against modification, disclosure, disruption, misappropriation, conversion, or destruction.
- Ensure compliance with the information protection laws and statutes of any country hosting Company’s business or information systems. (Interpretation of laws and statutes must come from Legal)
- Manage the protection of the company’s information systems in a way that ensures availability that is required of systems and information while remaining in conformity with the Company’s values.
- Ensure the company’s security standards and protocols remain updated and consistent with industry standards.

- Provide presentations at all levels of management to review strategies and associated risk analysis in developing and implementing an information protection system suited to business and operational need.
- Align the information protection program with other risk management programs including the enterprise risk management function and Internal Audit organization.
- Install and configure software and computer systems.
- Troubleshoot and resolve issues with software or hardware.
- Walk colleagues through steps to help them resolve their technical problems.
- Maintain procedures and reports that provide technical support to the entire organization.
- Analyze records and logs to spot underlying trends and potential issues.
- Support the implementation of new solutions or applications.
- Establish accounts for new users and assist with password or login problems.
- Test, evaluate, and make decisions about new technology for the business.
- Participate in business-wide meetings to provide insight into technical requirements.
- Security training selection and education would also include data/supplier catalogue

KNOWLEDGE & EXPERIENCE

- Bachelor's degree or higher in Computer Science, Information Technology, or other related field
- Certifications; one or more of CCISO, CISSP, CISM, CISA, CIPP, CSSLP
- 3-5 years of experience and proven record of success in information protection programs and security audit practices and IT support
- Working knowledge of IT systems security and technical security threats, working knowledge of industry standards
- Executive presence, strong influencing skills and the ability to convey a common sense of purpose and develop a culture in which different areas work together as a team with respect to issues of data security.
- Strong verbal, written and presentation skills in the area of explaining information protection policies, potential threats, and level of potential adverse impact to the company at all levels of the organization, record of effectively representing the company with clients, regulators and board as needed
- Builds positive relationships across organizations that foster a strong work environment