JOB TITLE: Cyber Security Data Protection Standards Manager

LOCATION: Bangalore

ABOUT UNILEVER:
Be part of the world's most successful, purpose-led business. Work with brands that are well-loved around the world, that improve the lives of our consumers and the communities around us. We promote innovation, big and small, to make our business win and grow; and we believe in business as a force for good. Unleash your curiosity, challenge ideas and disrupt processes; use your energy to make this happen. Our brilliant business leaders and colleagues provide mentorship and inspiration, so you can be at your best. Every day, nine out of ten Indian households use our products to feel good, look good and get more out of life – giving us a unique opportunity to build a brighter future.

Every individual here can bring their purpose to life through their work. Join us and you'll be surrounded by inspiring leaders and supportive peers. Among them, you'll channel your purpose, bring fresh ideas to the table, and simply be you. As you work to make a real impact on the business and the world, we'll work to help you become a better you.

ABOUT UNIOPS:

Unilever Operations (UniOps) is the global technology and operations engine of Unilever offering business services, technology, and enterprise solutions. UniOps serves over 190 locations and through a network of specialized service lines and partners delivers insights and innovations, user experiences and end-to-end seamless delivery making Unilever Purpose Led and Future Fit.

MAIN JOB PURPOSE:

Using a risk led and threat informed approach, this role will define and continually improve enterprise-wide data protection policies and standards in line with Unilever's risk appetite and cyber capabilities, ensuring alignment with controls frameworks which sit across IT and Data Privacy. With an aim to drive informed decision making and secure behaviour throughout the global business, this role is tasked with establishing the enterprise-wide data protection standards within cyber security. This role will be responsible for the definition and communication of these standards across Unilever. The role will also consult with other departments within Unilever who would be responsible for prescribed control implementation to ensure that they are actually deliverable within the Unilever environment. As part of the 2nd Line of defense, it is responsible for all data protection policies and standards within the cyber security standards framework.

KEY ACCOUNTABILITIES:

A vacancy exists for the Data Protection Standards Manager within Unilever's Cyber Security function. The successful candidate will be responsible for data protection standards across the whole of Unilever's global organisation. This role will report to the Director of Cyber Security Governance, Policies, and Standards.

Key areas under this role include:
The creation, maintenance and continuous improvement of our global data protection policies, standards, and controls covering the Unilever ecosystem, in close alignment with the Senior Policies and Standards Manager.
Ensuring the accepted control framework is implementable in our environment, in alignment with the Cyber Security Tech & Ops team, as well as the broader IT teams, on technology and process implementation for data identification, classification and protection.
Ensuring that the control framework is aligned with our risk assessment methodology and as such the implementation of any required changes are

coordinated across any dependent areas such as assurance and risk assessment.
Own and maintain processes to ensure all identified changes to data protection standards are collated, reviewed, accepted, signed off and communicated.
Monitoring NIST and other standard frameworks for updates and conducting gap analysis against our own data protection policies and standards.
Working with education, awareness, and engagement teams to ensure the organisation understands our data protection policies and standards, why they are important and how to get help in implementing them.
Partnering with UniOps and Data Privacy teams to ensure alignment across control frameworks and business changes.
Maintain awareness, and ensure visibility, of relevant regulatory compliance requirements, including triggering changes to standards, etc. where required.

The position will work with the wider Governance, Risk, Assurance, and Compliance team as well as our regional Business Information Security Officer teams globally to facilitate effective and consistent application of our data protection standards in support of implementing our global privacy policies, owned by Legal/Privacy.

Skills:
Excellent written and verbal communication skills and able to be understood by both technical and non-technical personnel.
Proven ability to lead, develop and motivate teams.
The ability to lead through accountability with delegated responsibilities.
Ability to manage conflicting priorities and multiple tasks.
Stakeholder management and interpersonal skills at both a technical and non-technical level.
Outstanding influencing ability.
Ability to work in a collaborative environment with international team members.
Outstanding critical reasoning and problem-solving skills – sticking to the problem until it is resolved.
Customer-orientated, whether responding to queries or delivering new services.
Skills in Programme and Project Management.

Experience:
The role holder will have previously held a role in Cyber Security.
Experience working with data and data protection in a cyber security context.
Understanding of and experience with global best practice standards (e.g. NIST, CIS, or ISO), Information Security standards and controls, and the three lines of defense model for appropriate segregation of duties and risk transparency.
International experience with Global 500 companies or similar preferred, but not required.
Experience and proven track record in Cyber Security including cyber risk management and governance.
Excellent strategic and operational business awareness, with a deep understanding of the key drivers, levers, issues, and constraints of digital businesses.
Experience within a customer focused environment.
Knowledge of the applications or the technical landscape within the domain and experience of delivering Cyber Security projects to its demands.

Candidates would be required to demonstrate the Unilever Standards of Leadership & live the Values through showing the following behaviours:

Agility – Flexes leadership style and plans to meet changing situations with urgency. Learns from the past, envisions the future, has a healthy dissatisfaction with the status quo.

Personal Mastery – Actively builds wellbeing and resilience in themselves and their team. Has emotional intelligence to take feedback, manage mood and motivations, and build empathy for others. Sets high standards for themselves and always brings their best self.

Passion for High Performance – Inspires the energy needed to win, generating intensity and focus to motivate people to deliver quality results at speed.

At HUL, we believe that every individual irrespective of their race, colour, religion, gender, sexual orientation, gender identity or expression, age, nationality, caste, disability or marital status can bring their purpose to life. So apply to us, to unleash your curiosity, challenge ideas and disrupt processes; use your energy to make the world a better place. As you work to make a real impact on the business and the world, we’ll work to help you become a better you!