Our TSA standards *Continued*

Enterprise Security

The importance of ensuring the security of our data and IT systems is paramount, as are the continual actions required to protect against ongoing threats. Intertek has robust measures in place to protect its people, processes and data.

Material topics

- **Customer and product responsibility**
- **Working with customers**
- **Compliance and legislation**
- **Privacy and security**

On our good-to-great journey we have developed our IT vision and strategy to systematically focus on security and reducing security risks. We proactively invest in advanced protection capabilities as hackers are sophisticated and become smarter. Effective detection and response capabilities ensure quick notification and we have robust processes in place to minimise any disruption to the business.

Through this programme, we support our operations and customers, facilitating growth and change with scalable, flexible IT solutions and services, as well as streamlining operations and improving processes and productivity to reduce costs of IT infrastructure and applications.

At Intertek we have adopted a risk-based security framework, based on international best practice, NIST CyberSecurity Framework. Our framework guides clear policies, standards and supporting guidelines, controls and hiring. We continue to innovate, enhancing service delivery and strengthening internal and external customer relationships to protect customer, employee and Intertek data.

There is regular reporting on progress of the security programmes to governance and oversight committees by our dedicated Head of Security, who leads a global team.

Awareness training

The Intertek CyberSecurity awareness training module was launched to all colleagues globally via our '10X Way!' learning platform. This training course, which is relevant to all employees, whether they collect and process personal data or not, was designed to provide useful information and tips to prevent cyber attacks when using Intertek technology at work or at home.

Our training is available in nine languages and has been rolled out across the Group. In 2020 awareness training was completed by 98% of employees (2019: 85%).

In 2020, we also made reporting email security issues even easier by introducing a link button on employee email systems. Employees can use this button to make a report directly to our CyberSecurity Hub.

Our TSA standards *Continued*

Enterprise Security

IT Security framework

With increasingly connected businesses and large supply chains it is imperative for businesses to approach Enterprise Security holistically; protecting our business from known threats, and strategically planning for emerging risks.

IDENTIFY

We develop a clear organisational understanding of risks to our systems, people and data, which enables us to prioritise efforts that are consistent with our risk management strategy and business needs.

PROTECT

We put in place appropriate safeguards to ensure delivery of critical services, including access control, staff awareness and training, and data security. These safeguards support our ability to limit or contain the impact of potential events.

DETECT

We define the appropriate activities for the timely discovery of the occurrence of security events. We monitor continuously and verify the effectiveness of protective measures including network and physical activities.

RESPOND

We ensure response planning processes are executed during and after an incident, so that we take appropriate action regarding situations and contain their impact. We also implement improvements, by incorporating lessons learned from current and previous detection/response activities.

RECOVER

We undertake appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an incident. Our recovery function ensures timely recovery to normal operations to reduce the impact from an incident.

Data protection

At Intertek, we believe all our people and all our customers have the right to data privacy. We have adopted the best practices and standards set out in the General Data Protection Regulation ('GDPR') across all of our markets and operations, and in relation to all individuals whose personal data we obtain and use (not just individuals in the EEA).

Our Group Data Protection Policy is aligned with the GDPR requirements to set out the minimum data protection standards we apply throughout our operations so that we use all personal data transparently, fairly and securely.

To ensure implementation, and to remain uncompromising on Quality and Compliance, our Core Mandatory Controls framework forms the mechanism to define, monitor and achieve consistently high standards.

Control and oversight is provided through our CyberSecurity Team, Group Legal & Compliance and the Internal Audit team. We have mandatory training on data privacy for all employees and global data breach response processes.

Zero

Number of complaints received from outside parties and substantiated by the organisation*

Zero

Substantiated complaints concerning breaches of customer data policy*

* As reported through our centralised system.

Our TSA standards *Continued*

Enterprise Security

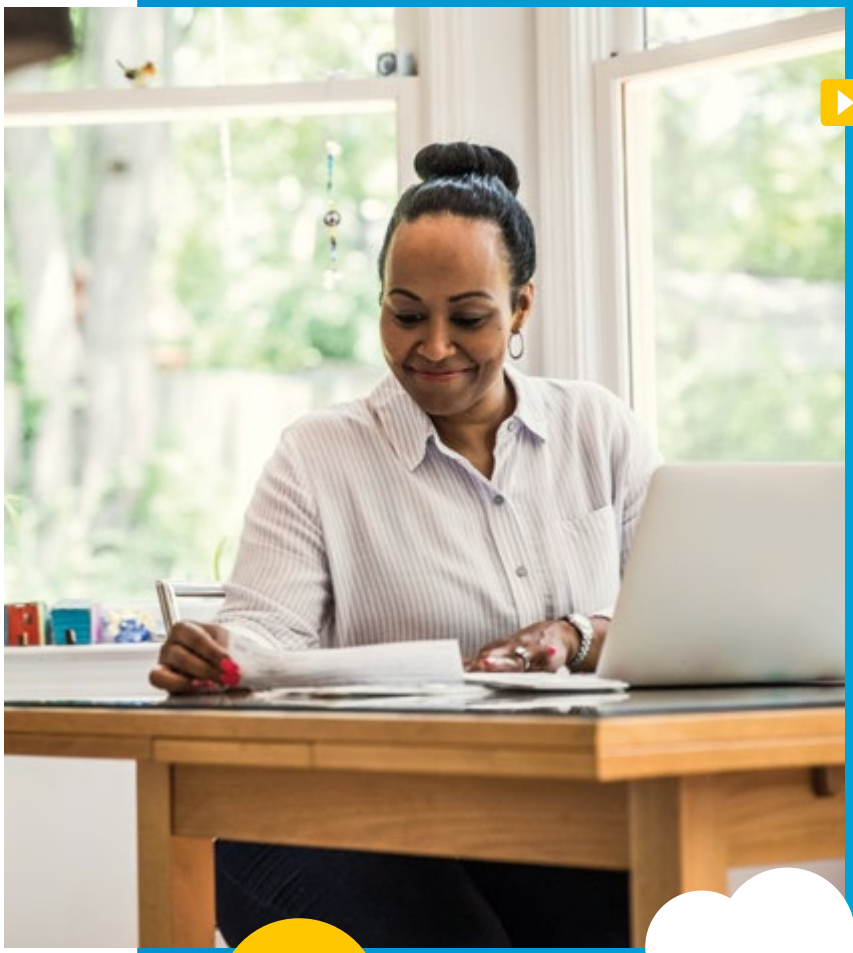
Physical assets

We place significant emphasis on the prevention, detection, management and response to security risks. We recognise that any breach would affect our ability to operate as normal and the integrity of our customers' information.

We have a framework and team in place to protect intellectual property, business services, personal information and customer data. Our Risk & Compliance team reviews the adoption and delivery of our Code of Ethics, including completion of training on the Code, and monitoring of activity including data privacy in all markets and functions.

Our global CyberSecurity team is trained to investigate and contain any personal data security incident and, together with the Legal & Compliance team, ensures any breach is reported within the timeframe required by local law.

Issues may also be raised through our Compliance hotline, via line managers, Legal representatives, Human Resources or the Compliance team. Audits and issues are reviewed, with remedial action being instigated as appropriate, including via the Audit Committee.



Case study

Catching phishers

In the very earliest days of the COVID-19 pandemic, Intertek's corporate CyberSecurity team was quick to identify and respond to a sudden increase in illicit phishing emails claiming to be from trusted authorities including the World Health Organization, national health bodies, government institutions and product vendors.

While our corporate online protection tools prevent most such malicious messages from being delivered, the team rapidly issued advice and guidance asking recipients to consider who might have sent a mystery email, not to click on attachments or links, and to forward it to them for analysis.