IT AND CYBERSECURITY POLICY STATEMENT

LUXFER HOLDINGS PLC

Lumns Lane
M27 8LN
Manchester
United Kingdom

www.luxfer.com

investor.relations@luxfer.com

LUXFER

July 7, 2021

LUXFER HOLDINGS PLC

IT AND CYBERSECURITY POLICY STATEMENT

As customer preferences and business-efficiency demands lead to a more connected and digitized world, cybersecurity and privacy risks have become critical business issues. Luxfer Holdings PLC ("Luxfer" or the "Company") understands the systemic nature of cybersecurity threats to the safety and security of our Company, customers, and employees. As such, Luxfer is committed to safeguarding and protecting our information technology ("IT") network, equipment, and systems against cybersecurity threats to ensure our future security and reduce risk.

Accordingly, we will continue to enhance ongoing governance, policies, and practices to address the following objectives:

- Ensure business continuity by protecting Luxfer's technology, data, intellectual property, and information assets;
- Increase cyber-resiliency and enhance controls for detecting and mitigating cybersecurity incidents;
- Safeguard the availability and reliability of Luxfer's network infrastructure, systems, and services;
- Ensure compliance with all applicable regulations and Luxfer policies, controls, standards and guidelines; and,
- Comply with requirements for confidentiality and privacy for Luxfer's customers and employees.

PURPOSE

Cybersecurity at Luxfer is a critical component of our success. The purpose of this Policy Statement is to enhance Luxfer's cybersecurity disclosure practices and describe the actions we take to ensure the security of our IT infrastructure, systems, and network.

BOARD OVERSIGHT AND MANAGEMENT

Approaching IT security with Board-level oversight and clearly defined roles and responsibilities.

As a part of its regular risk oversight, the Audit Committee of Luxfer's Board of Directors is responsible for overseeing cybersecurity, information security, and technology risk. The Audit Committee is comprised entirely of independent Non-Executive Directors based on NYSE listing standards, and the Committee Chair has earned the CERT Certificate in Cybersecurity Oversight. Additionally, three of Luxfer's Board members have information security experience. Luxfer's Senior Leadership provides regular reports on information security matters at least once quarterly to the Audit Committee, as it is their responsibility to oversee Management's actions to identify, access, mitigate and remediate material risk.

Luxfer's cybersecurity program is managed by our IT Steering Committee. Comprised of Group IT Managers and chaired by an executive leader, the IT Steering Committee maintains the vision, strategy, and operation of Luxfer's cybersecurity program. Group IT Managers, who have operational responsibility for the actions of the Committee, ensure the effective implementation of the Company IT policies. They also manage the local IT teams and ensure that they are appropriately supported. Local IT teams have the day-to-day responsibility for implementing and monitoring the operation of Company IT policies within their respective business units.

CYBERSECURITY RISK

Like all companies that rely on IT systems, Luxfer is exposed to cybersecurity risks.

We devote significant resources to network security, data encryption, employee training, monitoring of networks and systems, patching, maintenance and backup of systems and data. Additionally, we follow best practices for IT and data security, and are in the process of implementing DFARS/NIST 800-171 IT Security Standard for US Government Contractors. Although no cybersecurity incidents have been material to the Company to date, cyber-attacks are becoming more sophisticated and our IT network is still potentially vulnerable to threats and incidents in the future. While we maintain insurance coverage for cybersecurity and business continuity risks, there is no guarantee that all costs or losses incurred will be fully insured.

To assure long-term success, Luxfer is committed to discovering and preparing for all potential threats to our mission and values, including cybersecurity threats. We set out below certain mitigating actions that we believe help us manage our principal cybersecurity risks. Additional information about cybersecurity risks can be found on in our annual Form 10-K filed with the SEC.

RISK	RISK DESCRIPTION	MANAGEMENT OF RISK
Network and Systems	Luxfer's operations are increasingly dependent on IT systems and management of information, and a cyber-attack could inhibit our business operations including disruption to sales, production and cash flows.	Luxfer has a wide breadth of controls in place to protect against cyber-attacks including firewalls, threat monitoring systems, protected cloud architecture, and more frequent security patching. We have phased out vulnerable operating systems and updated legacy servers with advanced security. Applications that run and manage our core operating data are fully backed up.
Employee Error or Misuse	As cyber-attacks and phishing scams are becoming more advanced, employees may fail to recognize the signs of a cyber-attack or rely solely on the Company's IT defenses.	We have global policies covering IT security standards, annual training modules for employees. We also train our employees on cybersecurity through phishing simulations.
Third-Party Cybersecurity Measures	In part, we depend on the reliability of certain tested third parties' cybersecurity measures, including firewalls, virus solutions and backup solutions. Our business may be affected if these third-party resources are compromised.	Our IT Steering Committee performs thorough due diligence and risk analyses on third party vendors, verifying that sufficient security testing is performed on all software before installation on Luxfer's network. The IT Steering Committee also monitors and reviews access and permissions to all software and programs regularly.
Regulations	We are required to comply with the UK General Data Protection Regulation (GDPR) relating to the security of personally identifiable information that we process. A data breach can result in non-compliance with the GDPR, leading to fines or litigation.	We make every effort to comply with the GDPR and implement best practices including annual review of our Data Protection Policy. We also train employees to maintain secure systems, and access control measures, and regularly monitor and test our networks to protect data, payment information, and personally identifiable information.

COMPANY POLICIES

All Luxfer employees are responsible for IT safety and security.

Luxfer's Board of Directors have established strong IT and cybersecurity policies, procedures, guidelines and standards that are approved by Senior Leadership, reviewed at least once annually, and updated as needed. Our Policies apply to all employees, officers, consultants, contractors, vendors, interns, casual workers, agency workers, and anyone who has authorization to access Luxfer's IT network and systems ("employees").

IT ACCEPTABLE USE POLICY

Our IT and communications systems are intended to promote effective and responsible communication and working practices. Our comprehensive IT Acceptable Use Policy outlines the acceptable use of our IT and communications systems and the standards of conduct that employees are expected to observe when using these systems. The Policy iterates our standards for:

- IT equipment, data, and communications systems security
- Password requirements on computers and mobile devices
- Email security standards and requirements for safe use
- Detecting phishing emails and safe internet use
- Handling confidential information including customer data and payment information
- How to identify and report a potential data breach

BRING YOUR OWN DEVICE POLICY

While we support the use of Bring Your Own Device ("BYOD") technology such as smartphones and tablet computers to achieve business goals, we also understand that BYOD technology can represent an IT security risk if the appropriate security measures are not applied. Our BYOD Policy sets forth the expectations and standards that employees must follow when working from home or when connecting their own devices to the Luxfer network. In accordance with the Policy, devices must be pre-approved by the local IT team and must have security software applied to them before they are allowed to connect directly to the Luxfer network. The Policy also requires employees making use of BYOD to follow a specific set of technical requirements, use requirements, and application security measures.

DATA PROTECTION POLICY (GDPR)

We rely on centralized or local information technology networks and systems to collect, use, transmit, and store data, including proprietary business information and confidential information. We also have access to confidential or personal information that is subject to privacy and security laws, regulations, and customer-imposed controls. We are committed to complying with our obligations under applicable data protection laws and regulations, including the UK's General Data Protection Regulation (GDPR), and maintaining a clear and transparent dialogue about our use of personal data. The Policy iterates Luxfer's expectations, procedures, and security measures that apply to Luxfer employees who handle, process and transact with sensitive or personally identifiable information and data, including customer data and payment information.

EMPLOYEE TRAINING AND COMPLIANCE

Luxfer employees remain vigilant through cybersecurity training and awareness campaigns.

Our employees are a key line of defense against cybersecurity threats and malicious actors. In addition to our IT Policies, Luxfer has a comprehensive cybersecurity training and awareness program to educate employees on how to recognize cybersecurity threats, prevent cyber-related incidents, and how to report a potential threat or breach. Luxfer offers an online compliance training program which is mandatory for all Luxfer employees worldwide. It includes cybersecurity awareness and IT security trainings, along with other compliance and governance related topics. Within each training module, employees are required to review a Company IT policy applicable to the topic of the training, and attest that they have read, understood, and agree to comply with the Policy. Training topics for 2021 include Global Internet, Social Media & Electronic Communications; Privacy and Information Security; and Global Cybersecurity Basics.

In Focus: PHISHING

In 2018, Luxfer's IT Steering Committee launched an internal phishing simulation campaign to engage employees with cybersecurity, raise awareness, and educate employees on how to recognize and report phishing attacks. Through the simulation, we were able to test our employees' reaction to phishing emails and collect important metrics such as click rate. Data collection allowed us to pinpoint trouble spots and target additional trainings to specific teams or locations. To keep our employees on high alert, we increased the difficulty of the simulation emails to include social engineering and other deception techniques used in real-world phishing scams. Data collected from the phishing campaign is reported once quarterly to Luxfer's Senior Leadership Team and has proven to be an important supplement to our overall IT security training program.

Additional information about IT security and phishing is provided to employees through notices posted in readily accessible areas in our offices and breakrooms. We also communicate with our employees about IT security through internal "postcards" to provide timely reminders about IT safety and security topics.

STRONG ACCESS CONTROL PROCEDURES

Following best practices for access control and authentication.

Authentication and appropriate authorization are the hallmarks of a strong IT program, and we have implemented a set of controls through which we monitor access to our network and authenticate users. Access to our systems is limited to specific authorized users, devices, activities and processes. Access privileges and security levels (e.g., general user, administrator, IT administrator, etc) are limited based on the role of the individual and adhere to the "need-to-access" principle. Security levels are reviewed regularly by members of the local IT teams and any accounts are disabled and/or deleted in accordance with our IT Acceptable Use Policy.

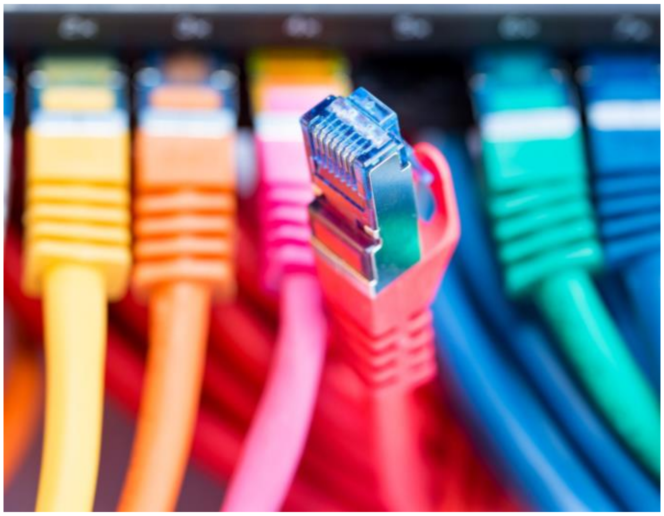
Pursuant to other Luxfer Policies, employees are required to use only unique, complex passwords that are at least 10 characters long and must be changed at least once annually. To carry out our legal obligations in our role as an employer, Luxfer uses automated software to monitor the use of our IT and communications systems, including email and instant messages. We also rely on other cyber tested third-party cybersecurity measures that will automatically detect and report any strange behavior in password activity to the Luxfer Group IT Managers, who will further investigate such reports and take the necessary action to resolve the potential threat.

STAKEHOLDERS WEIGHING IN

Luxfer remains committed to integrity and transparency in our cybersecurity disclosures.

Given the rapid shift to digital business in 2020, cybersecurity and data privacy are top priorities for Luxfer. Because the threat of a cyber-breach cannot be eliminated, we understand stakeholder's and shareholder's interest in our Company's cyber-resiliency. We believe in the importance of sufficiently informing the public about material cybersecurity risks and, should they occur, any material cybersecurity incidents affecting our Company. As such, Luxfer remains committed to transparency and increased disclosure regarding our cybersecurity practices.

In accordance with the SEC's *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* of 2018, we understand our obligations to disclose cybersecurity risks, material breaches, and the potential impact of breaches on the Company's finances and operations. While Luxfer has not experienced an information security breach in the last three years, we are fully committed to fulfilling our obligations under this Guidance so that investors can make the most risk-informed decisions possible.



Luxfer Holdings PLC
Lumns Lane, M27 8LN,
Manchester, United Kingdom

www.luxfer.com
investor.relations@luxfer.com