November 2018

CORPORATE SOCIAL RESPONSIBLITY

MTX2018-CSR

Contents

Revision History:

Document Revision	Change Request No.	Date	Change Owner
0	Original	06/11/2018	S. Tipper
1	47-2018	15/11/2018	S. Tipper

Document Scope:

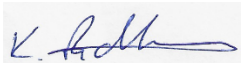
Addressing social issues responsibly is an important part of every Corporation's management system. Any Company intending to gain preferred supplier status approval to offer Mettex products or services will be asked to sign and return the last page within this document.

mettex
Braids, Strands & Flexible Connectors

Corporate Responsibility

The Mettex policy on Corporate Responsibility reflects a commitment to protecting future generations by acting responsibly with respect to the environment, sustainable development of the business and society. This policy is adopted throughout our business operations and across the supply chain which we believe is essential in developing business partnerships only with companies who share this goal of ecological, social and economic improvements for all.

This policy requires all suppliers of Mettex to submit self-assessment Code of Conduct responses and these must conform to the minimum requirements on both financial and non-financial factors to ensure future development of the business relationship, or risk removal from our approved supplier database. We believe this will protect us from any potential risk to our reputation and business and is essential to long term growth.

Signed 

Keith Ridley
Director

mettex
Braids, Strands & Flexible Connectors

Health & Safety Policy

Mettex Electric acknowledges its legal and moral responsibilities for ensuring the safety, health and welfare of its employees and any other persons whose health and safety may be affected by the Company's activities.

The Company recognises that having an effective policy in place which clearly identifies the Company's organisation and arrangements is essential to successful health and safety management.

A primary element of the policy is to prevent, so far as is reasonably practicable, injury or ill health, both to employees and other persons who may be affected by the activities of the Company.

The Company will strive to effectively communicate the policy and ensure that employees, and others who may be working on, using or visiting Company premises, fully understand the requirement on their part in carrying out the policy and that their activity is undertaken in a manner which does not expose themselves or others to risk.

Health and safety performance will be monitored as an agenda point at business meetings.

Adequate financial, human and other resources will be made available to ensure the effective implementation of the policy.

The provision of training for employees and the appropriate financial resource is an integral part of the policy.

The Company meets its requirement to appoint a *Competent Person* who will provide advice on safety matters and general health and safety assistance by the engagement of external competency.

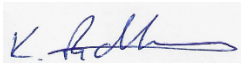
The requirement to communicate to and consult with employees is provided for by involvement of the workforce through shop floor meetings and the effective dissemination of information relating to healthy, safety and welfare matters.

The Company actively encourages participation in matters relating to health and safety. This includes ensuring an appropriate means for the reporting of safety and welfare issues by staff and suitable arrangements for joint consultation.

Appropriate action shall be taken should there be any breaches of established Health and Safety regulations or rules by any person(s).

The policy and its arrangements will be subject to monitoring and measurement in a structured, scheduled manner to determine performance against stated aims and objectives.

In addition to being reviewed by the senior management of the Company on an annual basis, the policy will be subject to continuous assessment, and as such will be amended should legislation, significant changes to working practices or new hazards necessitate this.

Signed 

Keith Ridley
Director

Environmental Policy

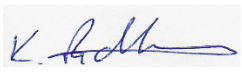
Our Aim

Mettex is committed to minimising the impact of its manufacturing processes on the environment and to continuously seeking improvements.

The key points in our strategy to achieve this are as follows:

- Promoting energy conservation
- Promoting careful avoidance of waste by evaluating operations and ensuring they are as efficient as possible
- Actively promoting recycling both internally and amongst customers and suppliers by utilising re-cycled materials and re-usable packaging where possible
- Meeting and exceeding all environmental legislation with regards to toxic emissions and pollution
- Creating an Environmental Management System accredited to BS EN 14001

This policy will be communicated to all staff and reviewed at regular intervals and will also be available to the general public on our company website, www.mettex.com

Signed 

Keith Ridley
Director

Ethical Sourcing Policy Conflict Minerals

Regulatory Information

On August 22, 2012, the U.S. Securities and Exchange Commission (SEC) published regulations implementing Section 1502 of the Dodd Frank Wall Street Reform and Consumer Protection Act governing Conflict Minerals. The Dodd Frank Act requires companies to perform due diligence on the source and chain of custody of Conflict Minerals to determine whether Conflict Minerals from the Democratic Republic of the Congo (DRC) or its adjoining countries are present in and are necessary to the functionality or production of our products.

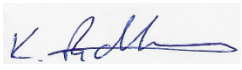
The SEC defines Conflict Minerals as tin (Sn), tungsten (W), tantalum (Ta) and gold (Au). These four minerals are collectively referred to as 3TG.

Our Aim

Mettex is committed to being an ethical business, ensuring all materials contained in its products are responsibly sourced and further by eliminating any supplier whose products contain conflict minerals sourced from any country that funds or supports inhumane treatment of its workers in violation of human rights.

Responsibility in the Supply Chain

Mettex requires all current and future suppliers to report using the CFSI template http://www.conflictfreesourcing.org/conflict-minerals-reporting-template/ and by working together seeks to achieve a conflict-free supply chain by only working with those suppliers whose businesses are compliant. This requirement has been added to the mandatory Supplier Approval Questionnaire within the Mettex Quality Management System.

Signed 

Keith Ridley
Director

REACH Statement

Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH)

Mettex Electric Co Ltd confirms that all products supplied by us fulfil the requirements stipulated in regulation (EC) 1907/2006 of the European parliament concerning (REACH)

As of the last update on the 27th June 2018, we understand from our suppliers that the products supplied to us do not contain substances of very high concern and do not foresee any problems in the continuing supply of these products.

If pre-registration of a substance is required we have further been assured that copies of pre-registration documents will be forwarded to us, in which case we will present these on request.

The Quality Manager is responsible for REACH related matters at Mettex.

Signed 

Keith Ridley
Director

RoHS & WEEE Statement

European Directives regarding the Restriction of Use of Hazardous Substances (RoHS) and Waste Electrical and Electronic Equipment (WEEE)

With reference to compliance to the recast RoHS 3 Directive 2015/863, all copper products supplied by Mettex are compliant with new legislation. Although copper contains very low levels of both lead and cadmium, these are naturally occurring elements and are not added to the products intentionally. Please see the data sheet below for copper rod used in the manufacture of copper wire purchased by Mettex.

Table of chemical analysis for copper (taken from BS EN 1977)
Cu-ETP1 / CW003A – material supplied by rod manufacturers

Element	Max (%)
Cu	
Ag	0.0025
As	0.0005
Bi	0.00020
Cd	
Co	
Cr	
Fe	0.0010
Mn	
Ni	
O	0.040
P	
Pb	0.0005
S	0.0015
Sb	0.0004
Se	0.00020
Si	
Sn	
Te	0.00020
Zn	

(As+Cd+Cr+Mn+P+Sb) maximum 0.0015%
(Bi+Se+Te) maximum of 0.0003%, of which (Se+Te) maximum of 0.00030%
(Co+Fe+Ni+Si+Sn+Zn) maximum 0.0020%

Signed 

Keith Ridley
Director

Proposition 65 – Safe Drinking Water and Toxic Enforcement Act of 1986

Mettex Electric Co Ltd confirms that all products supplied by us meet the thresholds of the Safe Drinking Water and Toxic Enforcement Act of 1986.

As of the last update on the 25th May 2018, we understand from information provided by our suppliers that the materials supplied to Mettex do not contain or exceed the levels of chemicals listed in Proposition 65.

If further information is required regarding this declaration, please contact the Quality Team at Mettex.

Signed 

Keith Ridley
Director

Data Security Policy

Overview

Mettex Electric Co Ltd is entrusted with the responsibility to provide appropriate protection against theft of data and malware threats, such as viruses and spyware applications and minimise the threat of unauthorised access to its data.

This policy applies to equipment owned and/or operated by Mettex Electric Co Ltd, and to employees connecting to any owned network domain.

Network/Server Security

Server Configuration Guidelines

The most recent security patches must be installed on the system as soon as practical.

Servers should be physically located in an access-controlled environment.

Security-related Events – Any suspicious events to be reported to the IT management. Corrective measures will be prescribed as needed.

Router Security

The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.

Each router must have the following statement posted in clear view: "UNAUTHORIZED ACCESS

TO THIS NETWORK DEVICE IS PROHIBITED. "

Server Malware Protection

All servers including mail servers must have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system.

Backup Procedures

Backup software shall be scheduled to run nightly to capture all data from the day.

Backup logs are to be reviewed to verify that the backup was successfully completed.

Finance Manager to carry out backups each day, if not available, Finance Admin should oversee the process.

Backup data storage from the previous night shall be removed from Mettex premises on a daily basis.

Lakeview Computers to Test restoration process regularly.

Workstation Security

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information is restricted to authorized users. Mettex Electric Co Ltd will implement safeguards for all workstations that access electronic confidential information to restrict access to authorized users. Appropriate measures include:

Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.

Complying with all applicable password policies and procedures.

Ensuring workstations are used for authorized business purposes only

Never installing unauthorized software on workstations.

Storing all confidential information on network servers.

Securing laptops that contain sensitive information by storing in our locked server room.

Ensuring that all servers use a surge protector (not just a power strip) or a UPS (battery backup).

Software Installation

Employees may not install software on computing devices operated within the network. Software requests must first be approved by the IT department.

This policy covers all computers, servers, and other computing devices operating within Mettex Electric Co Ltd network.

Anti-Virus Protection

Anti-Virus - All computers must have ESET Endpoint anti-virus software installed and this must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited. All computers must have I Critical installed to protect emails and Web Critical to protect whilst using the internet or internet-based programmes.

Password Security

Standards - All users at Mettex Electric Co Ltd should select strong passwords. Strong passwords should contain four of the five following character classes:

1. Lower case characters
2. Upper case characters
3. Numbers
4. Punctuation

5. “Special” characters (e.g. @#$%^&*()_+|~-=\`{}[]:”;’<>/ etc)

Security Protective Measures

Do not share passwords with anyone, all passwords are to be treated as sensitive, confidential information. Forced password changes will occur every 3 months.

Always decline the use of the “Remember Password” feature of applications.

General Use and Ownership

While Mettex Electric Co Limited networked administration will provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Mettex Electric Co Ltd

Any information that users consider sensitive or vulnerable to be secured.

All PCs, laptops and workstations should be secured by logging off when unattended.

Unacceptable Use - The following activities are, in general, prohibited. The lists below are by no means exhaustive, but provide a framework for activities which fall into the category of unacceptable use.

Under no circumstances is an employee authorized to engage in any activity that is illegal while utilizing Mettex Electric Co Ltd owned resources.

Violations of the rights of any person or Firm protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of “pirated” or other software products that are not appropriately licensed for use by Mettex Electric Co Ltd

Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

Using a computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.

Making fraudulent offers of products, items, or services originating from any Mettex Electric Co Ltd account.

Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.

Port scanning or security scanning is expressly prohibited unless prior notification to the IT department is made.

Executing any form of network monitoring which will intercept data not intended for the employee's host.

Circumventing user authentication or security of any host, network or account.

Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet.

Providing information about, or lists of employees to parties outside.

Visitors who require internet network access will need permission from the IT department. Visitor use of employee credentials is not permitted under any circumstances.

Wireless Access including Home Wireless Devices must be installed, supported, and maintained by the IT department and maintain a hardware address (MAC address) that can be registered and tracked.

Mobile Device Encryption - all mobile devices containing stored data owned by Mettex Electric Co Ltd must use an approved method of encryption to protect data. Mobile devices are defined to include laptops, tablets, and smartphones.

E-mail

Prohibited Use - Mettex Electric Co Ltd e-mail system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any e-mails with this content from any employee should report the matter to their supervisor immediately. The following activities are strictly prohibited, with no exceptions:

Sending unsolicited e-mail messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (e-mail spam).

Any form of harassment via e-mail and telephone, whether through language, frequency, or size of messages.

Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.

Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

Personal Use - Using a reasonable amount of Mettex Electric Co Ltd resources for personal e-mails is acceptable, but non work related e-mail shall be saved in a separate folder from work related e-mail. Sending chain letters or joke e-mails from a Mettex Electric Co Ltd e-mail account is prohibited.

These restrictions also apply to the forwarding of mail received by an employee.

Users to exhibit extreme caution when open email and attachments from unknown sources.

E-mail Retention - emails should not be retained for longer than is necessary. Any sensitive emails should be stored on the secure network drive G.

Employees shall have no expectation of privacy in anything they store, send or receive on the Firm's e-mail system. Mettex Electric Co Ltd may monitor messages without prior notice.

Mobile Computing and Storage Devices

Mobile computing and storage devices include, but are not limited to: laptop computers, plug-ins, USB port devices, CDs, DVDs, flash drives, smartphones, tablets, wireless networking cards, and any other existing or future mobile computing or storage device. Only equipment owned by Mettex Electric Co Ltd may connect to or access the company's information systems

Mobile computing and storage devices are easily lost or stolen, presenting a high risk for unauthorised access and introduction of malicious software to the network, these risks must be mitigated to acceptable levels as follows.

Any employees issued with company owned flash drives, must sign the equipment out when removing it from the company premises and sign it back in on its return. A log of users and their equipment ID is kept on the company G drive under Flash Drive Log, MTX2018-FDL.

Databases or portions thereof, which reside on the network shall not be downloaded to mobile computing or storage devices.

Report lost or stolen mobile computing and storage devices to the IT department as soon as possible.

Virtual Private Network (VPN)

Only approved employees and authorized third parties may utilise the benefits of VPNs.

It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.

VPN gateways will be set up and managed by Lakeview Computers.

Employee Termination

An employee's credentials and access to all systems shall be deactivated immediately upon termination of employment.

Any employee in possession of any company portable devices shall return such devices before exiting the premises on their final day of employment.

Visitors who require internet network access will need permission from the IT department. Visitor use of employee credentials is not permitted under any circumstances.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Signed 

Keith Ridley
Director

Anti-Bribery Policy

In line with the 2010 Bribery Act that came into force in July 2011, Mettex is committed to a zero-tolerance policy on any matters of bribery. This is generally defined as giving someone an item of value, may be financial or of other benefit, to influence or reward that person to perform an action in return.

Potential risks to bribery have been identified and scored accordingly, actions to address these risks have been created and these actions will be monitored & reviewed annually to ensure they are sufficient in dealing with the risks identified.

This policy will be communicated to all staff and reviewed at regular intervals and will also be available to the general public on our company website, www.mettex.com

Signed 

Keith Ridley
Director

Counterfeit Parts Prevention Policy

Counterfeit parts can have a serious effect on the safety, performance and reliability of products. To prevent any counterfeit parts entering production, all suppliers must gain approval before providing Mettex with any parts, Certificates of Conformity must accompany all deliveries and full traceability to source shall be attainable.

Internally, Mettex monitors industry alerts and when required acts to address these risks. Continual improvement of the quality management system enables us to make certain the processes yield the outputs required.

This policy will be communicated to all staff and reviewed at regular intervals and will also be available to the general public on our company website; www.mettex.com

Signed 

Keith Ridley
Director

Whistleblowing/Escalation Policy

At Mettex, keeping the channels of communication open at all times is essential to the successful feedback of information throughout the Company. This policy emphasises these channels are open to all employees in the event that there is the need to "make a disclosure" or "blow the whistle" on any wrong doing typically, but not always, observed within the Company.

To be covered by the whistleblowing law, located in Employment Rights Act 1996 (as amended by the Public Interest Disclosure Act 1998), the disclosure being made must firstly be in the interest of the public. Secondly the employee must reasonably believe the disclosure displays past, present and future wrongdoing falling into one of the below categories:

- Failure to comply with obligation set out in law
- Endangering of a person's health & safety
- Damage to the environment
- Miscarriages of justice
- Criminal offense, for example fraud
- Concealment of any wrongdoing

If an employee feels the need to blow the whistle, this wrong doing can be communicated to a person in management, the Mettex whistle-blower champion or a prescribed person (*Whistleblowing: list of prescribed people and bodies*, can be found at https://www.gov.uk/government/publications/blowing-the-whistle-list-of-prescribed-people-and-bodies--2). An employee can keep their confidentiality by making an anonymous disclosure however, they may not receive feedback and any action taken can be limited. If feedback is given, this can be done by making a telephone appointment or using an anonymous email address.

It should be emphasised that; no evidence needs to be presented when making a disclosure and any victimisation of a whistle-blower is deemed as totally unacceptable by the Company. For further information regarding the procedure, please see "Grievance Procedure" in the Company Contract.

This policy will be communicated to all staff and reviewed at regular intervals and will also be available to the general public on our company website, www.mettex.com

Signed 

Keith Ridley
Director

Supplier Agreement to Mettex CSR Policies

Mettex takes Corporate Social Responsibility seriously and expects our preferred suppliers to act accordingly.

Please sign below to agree acceptance of our CSR policies and return a scanned signed copy of this page to Mettex using the email address elaine@mettex.com

Policies included in MTX2018-CSR Revision 1:

- ☑ Corporate Responsibility
- ☑ Health & Safety Policy
- ☑ Environmental Policy
- ☑ Ethical Sourcing Policy Conflict Minerals
- ☑ REACH Statement
- ☑ RoHS & WEEE Statement
- ☑ Proposition 65 – Safe Drinking Water and Toxic Enforcement Act of 1986
- ☑ Data Security Policy
- ☑ Anti-Bribery Policy
- ☑ Counterfeit Parts Prevention Policy
- ☑ Whistleblowing/Escalation Policy

Company Name: …….

Print Name: …….

Position: …….

Signature: …….

Date: …….