

COMPANY DIRECTIVE WHISTLEBLOWING

Definitions

The Company = Mitsubishi Electric Europe B.V., Mitsubishi Electric Russia and Mitsubishi Electric Turkey

EEA = European Economic Area

Employee and/or Worker = an individual who has entered into or works under a contract of employment with the Company, or any Contractors, Consultants, Temporary agency personnel or a person engaged to provide similar services to the Company and who has direct access to the Company's internal IT systems and reporting processes.

EU = European Union

External Stakeholder = with the exception of Employees and/or Workers of the Company, this includes any person working in the private or public sector who interacts with the Company in a work-related context including: workers, civil servants, self-employed individuals, shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees, and any persons working under the supervision and direction of contractors, subcontractors and suppliers. The term shall also include any individuals whose work-related interactions with the Company take place during a recruitment process or other pre-contractual negotiation, or whose work-related interactions took place during a contractual relationship with the Company which has since ended. Where relevant, third persons with a connection to the aforementioned individuals (such as their colleagues or relatives, individuals providing them with assistance, or legal entities connected to them) may also qualify as an External Stakeholder.

MEU = Mitsubishi Electric Europe B.V.

MER = Mitsubishi Electric Russia

METR = Mitsubishi Electric Turkey

Relevant Breach = Possible breaches of EU law in the areas listed in Article 2(1) of the Directive, including: public procurement, financial services, prevention of money laundering, terrorist financing, product safety, transport safety, environmental protection, nuclear safety, feed and food safety, animal health and welfare, public health, consumer protection, data privacy and the security of networks and information systems. Relevant Individuals should refer to any branch level measures for any additional areas of law that may be a Relevant Breach in the Relevant Individual's country.

Relevant Individual = An Employee, Worker or External Stakeholder

Policy = Means this Company Directive Whistleblowing, updated on 1st December 2021

The Directive = Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019

Purpose

It is important to the business that any fraud, misconduct or wrongdoing by employees or officers of the Company is reported and properly corrected. The Company therefore encourages all Relevant Individuals to raise any concerns which they may have about the conduct of others in the business or the way in which the business is run. This Policy sets out the procedure by which Relevant Individuals may raise any concerns that they have and how those concerns will be dealt with.

Scope

This Policy has been prepared to align with The Directive. As such, some aspects of this Policy will not apply to branches or representative offices of MEU, MER and/or METR which are located outside the EU/EEA, as noted below. In particular, branches or representative offices of MEU outside the EU/EEA, MER and/or METR may not be required to follow those parts of this Policy which relate to reporting by External Stakeholders. It is also possible that some complaints or reports relating to purported breaches of legal obligations may not qualify as Relevant Breaches and may not fall within the scope of this Policy.

This Policy applies to all present and former Employees and/or Workers. It also applies to External Stakeholders, to the extent that they are seeking to report a Relevant Breach.

This Policy does not form part of any contract of employment or otherwise have contractual effect.

Application

The application of this Policy is as follows.

Within the section “Principles” below:

- i. The sub-section titled “Internal Reporting” applies to all present and former Employees and/or Workers of the Company in all its territories.
- ii. The sub-section titled “External Reporting” applies to all External Stakeholders.

This Policy may be amended from time to time and may be supplemented with additional branch level measures to account for the way that national laws implement the Directive.

MEU branches may also implement additional or equivalent practical measures in order to facilitate reporting, e.g. utilisation of the services of entrusted third parties. Such measures may operate in addition to, or in place

of, the internal reporting measures described in this Policy. However, any entrusted third parties must operate in line with the aims and objectives of those measures and to the same standard as described in the Directive.

Principles

All Relevant Individuals should be aware of the importance of preventing and eliminating wrongdoing at work or in a work-related context. They should be watchful for illegal or unethical conduct and report anything of that nature that they become aware of.

- a. This Policy provides protection for Relevant Individuals who raise concerns about a possible Relevant Breach. This protection will apply where a Relevant Individual has reasonable grounds to believe that a Relevant Breach is being, has been, or is likely to be committed.

It is not necessary for the Relevant Individual to have proof that a Relevant Breach is being, has been, or is likely to be, committed – a reasonable belief is sufficient. However, the Relevant Individual is recommended to provide the Company with any *prima facie* evidence supporting their concern so that the Company may conduct a more exhaustive investigation. The Relevant Individual should not try to build a detailed case by conducting their own private investigation; it is the Company's responsibility to ensure that an investigation takes place against concerns that are raised along with *prima facie* evidence. In cases where no *prima facie* evidence is provided, the Company will apply its discretion as to the conduct of any further investigation, depending on the nature of the Relevant Individual's concern.

Any concern raised under this procedure will be investigated thoroughly, promptly and confidentially, with appropriate feedback provided to the Relevant Individual. Any feedback provided will be limited as necessary, in line with the Company's personal data protection and confidentiality obligations towards other Relevant Individuals.

Internal Reporting

Internal reporting refers to a report regarding a possible Relevant Breach made within the Company, by any Relevant Individual who is an Employee and/or Worker. It does not refer to any report made by an External Stakeholder.

Procedure for Internal Reporting

1. The Employee and/or Worker should in the first instance raise their concerns with the relevant line manager. Concerns may be raised in writing or orally. In the case that the Employee and/or Worker

either (1) believes their line manager to be involved in the Relevant Breach, or (2) for any other reason does not wish to approach their line manager, then the Employee and/or Worker should proceed to Step 3 below.

2. The line manager will acknowledge receipt of the report as soon as possible and within no more than seven days and will then arrange an investigation of the matter (by immediately escalating the report to the correct person). Depending on the circumstances, the investigation may involve the Employee and/or Worker who made the report and any other Employees and/or Workers involved in the matter being requested to provide a written statement. Any investigation will be carried out in accordance with the principles set out above. The statement of the Employee and/or Worker who raised the concern(s) will be taken into account, and that individual will be asked to comment on any additional evidence obtained. The line manager shall maintain appropriate lines of communication with the Employee and/or Worker who raised the concern(s) and may seek further information from them as required. The line manager (or the person who carried out the investigation) will then report to the Branch President via the senior Human Resource Manager, who will take any necessary action including reporting the matter to any appropriate government department or regulatory agency. If disciplinary action is a possible outcome, the senior Human Resources Manager will start the disciplinary procedure.

Within three months the Employee and/or Worker will then be informed of any action taken, the status of any internal investigation and the outcome of that investigation. If no action is to be taken, the reason for this will be explained. Where the case requires additional time to complete the investigation the Employee and/or Worker will be updated as such within this three-month period and informed of the expected date of completion of the final report.

Any reporting of a possible Relevant Breach will be treated with the strictest confidence and access to the report shall be appropriately limited on a 'need-to-know' basis. As far as possible, the Employee and/or Worker's identity will be protected and not disclosed without their prior consent.

3. If the Employee and/or Worker is concerned that their line manager is involved in the Relevant Breach, or for any other reason does not wish to approach their line manager then that individual should inform the senior local or Corporate Human Resource manager who will assume the responsibilities of the line manager that are set out in step 2 above as required.
4. As an alternative to the options stated above, in some circumstances the Employee and/or Worker may submit a concern about a Relevant Breach using the MEU-CORP Internal Whistleblowing Hotline (the '**Internal Hotline**'). The procedure for using the Internal Hotline is set out in Appendix 1 below.

External Reporting

External reporting refers to a report regarding a possible Relevant Breach made by a Relevant Individual who is an External Stakeholder. It does not primarily refer to any report made by an Employee and/or Worker. Any External Stakeholders (including, for the avoidance of doubt, any individuals who are former Employees and/or Workers) who do not have access to MEU's internal reporting systems may also use this procedure to make a report.

Procedure for External Reporting

External Stakeholders may submit a concern about a Relevant Breach using the MEU-CORP External Whistleblowing Hotline (the '**External Hotline**'). The procedure for using the Internal Hotline is set out in Appendix 2 below.

The law recognises that in some circumstances it may be appropriate for any Relevant Individual to report their concerns regarding a Relevant Breach to an external body such as a regulator. It will very rarely if ever be appropriate to alert the media. We strongly encourage all Relevant Individuals to seek advice before reporting a concern to anyone external.

Further information in relation to the processing of reports received from the Internal and External Hotlines, including an explanatory flow-chart, is set out in Appendix 4 below.

Protection from retaliation

Any Relevant Individual who, having a reasonable belief in a possible Relevant Breach at the relevant time, raises any concern about such a Relevant Breach and raises this concern using the appropriate routes, as described under 'Internal Reporting' or 'External Reporting' above has the right to be protected from all forms of actual, threatened, or attempted retaliation. Retaliation in this context can take many forms and can include, but is not limited to, the following acts:

- suspension, lay-off, or dismissal;
- demotion;
- withholding of promotion or training;
- a negative performance assessment of employment reference;
- imposition of a disciplinary measure or penalty; and
- any other form of coercion, intimidation, harassment or disadvantageous or unfair treatment.

A Relevant Individual may consult a legal advisor to obtain advice on the procedures and remedies available to them, on their protection against retaliation and their rights as a whistleblower.

Where wrongdoing is discovered as a result of any investigation under this procedure the Company's disciplinary procedure will be utilised, in addition to any appropriate external measures e.g. referral of the matter to the relevant authorities. Any instruction to "cover up" or otherwise conceal wrongdoing is regarded as a disciplinary offence. If a Relevant Individual is told not to raise or pursue any legitimate concern by an Employee and/or Worker, even by a person in authority such as their line manager, they should not agree to remain silent but should report their concern to a person with management responsibility. Where a concern regarding a Relevant Breach is raised without a reasonable belief in its truth at the time that the concern is raised (including scenarios where a concern is raised in a malicious or false manner), this may (depending on the particular circumstances) be regarded as a disciplinary offence.

Reports received outside the channels described above

The reporting channels for internal and external reporting noted above are the mechanisms that MEU has introduced in order to be able to meet its legal obligations under the Directive and relevant national law.

As such MEU cannot guarantee that the obligations in terms of time limits set out in the EU Whistleblower Protection Directive and any relevant national law will be met in any case where a different mechanism is used by a Relevant Individual to make a report.

MEU Employees who are recipients of an internal report outside the stated channels shall first discuss with and forward to the HR GM (most senior member of HR) at that branch. The HR GM will then treat the report as if it had been received by themselves as at "Procedure for Internal Reporting" Step 3 above.

If a report outside the stated channels is received from an external Relevant Individual then the recipient of the report will again forward to the HR GM, who will liaise with the branch legal department in order to ascertain the correct course of action.

Data Protection and Information Security

The Company maintains full compliance with the General Data Protection Regulation ('GDPR') of the EU and its national implementing legislation in all territories of operation in line with the MEU Data Protection Code of Conduct, and also with the national data protection regulations of all other territories in which it operates. All personal data received as part of a report into a possible Relevant Breach will be treated in accordance with the Company's Data Protection policies and in line with relevant local laws. Reports will be held securely as

“Secret” documents under the terms of the Company’s Information Security Management protocols, in order to maintain the highest standard of security and confidentiality.

Appendix 1 - Operation of the Internal Hotline

NB - The Internal Hotline does not apply to branches that have already implemented an external whistleblowing measure utilising the services of a lawyer, and/or as specifically negotiated and agreed by that branch's national Works Council. In cases where the use of the Internal Hotline does not apply for this reason, Employees and/or Workers of that branch should instead refer to the steps listed in the Policy above.

Operation of MEU-CORP Whistleblowing Internal Hotline

Constituting an additional route for submitting concerns about a Relevant Breach, the Internal Hotline is intended to serve as a line of reporting outwith the branch-level management reporting structure. It is a supplementary method for reporting any possible Relevant Breach which an Employee and/or Worker may be concerned with.

Raising a concern through the Internal Hotline

In order to submit any concern, the Employee and/or Worker should access via MEU's intranet pages on Sharepoint where there is a link to the 'MEU-CORP Whistleblowing Hotline'.

Once the employee clicks on this link, a new window with the report form shall open:

From:
Topic:
Message:

All lines in the form should be filled out. If the Employee and/or Worker wishes to submit any concern on an anonymous basis, they may do so by leaving the line "From" blank. However, we encourage Employees and/or Workers to identify themselves without any fear of retaliation and refer them to the protections detailed in the Policy. In general, it is less likely that an investigation can be pursued thoroughly in response to an anonymous concern.

Reports concerning possible Relevant Breaches may be submitted in the recognised national languages of the branch or branch office concerned as appropriate. Please note that reports submitted in languages other than English may require some additional time for a response due to the requirement for professional translation. Responses to reports cannot be guaranteed to be provided in the same language as the report

and may be provided by MEU-Corp in English.

The reporter should describe the incident by answering five basic questions:

- What happened?
- Where?
- When?
- Why?
- Who did it?

Appendix 2 - Operation of the External Hotline

External Stakeholders (including, for the avoidance of doubt, any individuals who are former Employees and/or Workers) who do not have access to MEU BV's internal IT systems may make a report regarding a possible Relevant Breach following the procedure outlined below.

1. Access the MEU Whistleblowing internet page.

This page can be found at: <https://emea.mitsubishielectric.com/>

2. Follow the instructions given at the above internet page.
3. Alternatively, reports may be submitted in written form to:

The Compliance Committee, MEU Corporate Office, 1 Harman House, Uxbridge, United Kingdom UB8 1QQ.

We encourage External Stakeholders who submit a report to identify themselves without any fear of retaliation and refer them to the protections detailed in the Policy. Should an External Stakeholder prefer to submit their concerns on an anonymous basis, they may do so. In general, it is less likely that an investigation can be pursued thoroughly in response to an anonymous concern.

Reports concerning possible Relevant Breaches may be submitted in the recognised national languages of the branch or branch office concerned as appropriate. Please note that reports submitted in languages other than English may require some additional time for a response due to the requirement for professional translation. Responses to reports cannot be guaranteed to be provided in the same language as the report and may be provided by MEU-Corp in English.

The reporter should describe the incident by answering five basic questions:

- What happened?
- Where?
- When?
- Why?
- Who did it?

Appendix 3 - Processing of reports received from the Internal and External Hotlines

Processing

In order to guarantee professional consideration of all messages received, MEU-CORP has established a Compliance Committee (hereinafter the “**Committee**”). The Committee consists of MEU-CORP HR GM, MEU-CORP Legal GM, MEU-CORP Audit GM, MEU-CORP Finance GM, and the General Counsel MEU-UK. Administrative assistance to the Committee may be provided by a member of MEU Corporate Office staff.

All reported concerns regarding possible Relevant Breaches are handed over directly to the members of the Committee. Having analysed the reported issue, the members of the Committee may use one of three solutions:

- a) Reject the concern and decide that further processing of the concern shall be discontinued without explanation, for example in the case of insufficient information from the reporter.
- b) Accept the concern for further consideration. Investigate it via the Committee and prepare a report of the findings of this investigation together with recommendations for resolving the issue.
- c) Accept the concern for further consideration. Investigate it with the involvement of third parties, including outside experts (e.g. lawyers, consultants specialized in a particular area of law/business), and prepare a report of the findings of this investigation together with recommendations for resolving the issue.

At any stage of the process, should the Relevant Individual request a meeting with the investigator or the investigating team then a meeting will be granted with at least one member of that team.

Please refer also to the ‘MEU-Corp Whistleblowing Hotlines Flow-chart’ below.

Response and Reporting

Upon the completion of the steps outlined above the Committee will submit a report to the MEU President.

If a concern made via either the Internal or the External Hotline was accepted, the Committee shall also submit a report to the President(s) and (where relevant) the CCO(s) of the MEU Branch(es) concerned. In the case of an anonymous report, the Committee shall send a report to both the President(s) and CCOs of MEU Branch(es) concerned.

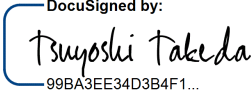
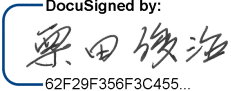
The report shall contain a summary of the concern received from the Relevant Individual, the results of the investigation conducted by the Committee, and recommended steps to resolve the issue.

Where a Relevant Individual provides contact details, and whichever process they use to raise a concern regarding a possible Relevant Breach to the Company, the concern made will be acknowledged by The Committee as soon as possible and certainly within no more than seven days of receipt. The Committee shall maintain appropriate lines of communication with the Relevant Individual who raised the concern(s) and may seek further information from them as required. Within three months the Relevant Individual will then be informed of any action taken, the status of any internal investigation and the outcome of that investigation. If no action is to be taken, the reason for this will be explained. Where the case requires additional time to complete the investigation the Relevant Individual will be updated as such within this three-month period and informed of the expected date of completion of the final report.

As far as possible, MEU will maintain the confidentiality of the report and the anonymity of Relevant Individuals at all stages of the process.

In the process of reaching any conclusions in respect of a report made under the Directive, the responsible management will also take into account MEU's Risk Management Policy (and/or any other policy directly relevant to the matter under investigation) as appropriate in each case.

Approval matrix

	Revised and Updated by	Approved by
Signature		
Name	T. Takeda	S. Kurita
Title	MEU-Corp HR General Manager	MEU President & CEO
Date		

Issue history:

First issued: 16 April 2010

Revised and updated: 09 February 2018

Revised and updated: 01 December 2021

Revised and updated: 07 December 2022