Requirements for Suppliers in Euroclear Premises

Anyone working at Euroclear must adhere to the code of business conduct on which principles these requirements have been drawn.

If you have any questions relating to these requirements, please contact the compliance department (compliance@euroclear.com).

1. Ethical Conduct

1.1 Abide by high standards of fairness, honesty and integrity.

1.2 Respect and obey the spirit and the letter of the laws and regulations of the jurisdictions where we operate.

1.3 Ensure that communications with Euroclear's clients and shareholders are complete, timely, straightforward and fair.

1.4 Do not discriminate against anyone for reasons which include – but are not limited to - age, race, sex, religion, disability or sexual orientation.

1.5 Do not act in a way that can be classified as:

- **a.** violent; or
- **b.** sexual harassment (verbal, non-verbal or physical behaviour of a sexual nature); or
- **c.** moral harassment (abusive and repeated conduct of any origin which manifests itself in particular by unilateral behaviour, words, intimidation, acts, gestures and writings, whose purpose or aim is to harm the personality, dignity, physical or psychological integrity of someone); or
- **d.** bullying behaviour. Bullying is defined as any unsolicited or unwelcome act that humiliates, intimidates or undermines the individual involved.

1.6 Do not consume alcohol on Company premises without the appropriate permission.

1.7 Do not take, buy, sell or be in possession of drugs which are not for medical purposes on Euroclear premises.

1.8 Deal with Euroclear's regulators in a lawful, open and co-operative manner.

1.9 Do not commit or conceal fraudulent or illegal acts and report suspicion or evidence of fraudulent activities to your Euroclear contact point.

1.10 Neither you, your family members or other relatives must accept gifts offered because of your position at Euroclear with a retail value greater than EUR 100 (or equivalent) without prior approval from your Euroclear contact point. Cash offers, regardless of amount, must always be refused. Ordinary meal invitations in the usual course of business may be accepted.

1.11 Refer all press and media inquiries, including requests to write an article or to be interviewed about your experience at Euroclear or any Euroclear-related business developments, to the Euroclear corporate communications team before engaging in dialogue with a journalist.

1.12 Adhere to Euroclear's dress code when working on Euroclear premises, which is smart casual, but must be standard business attire when meeting with external clients on the premises or during external business meetings.

1.13 Never sign an official document that could be binding for Euroclear (e.g. invoices, contracts with providers, etc.) or request quotations from vendors on behalf of Euroclear.

1.14 Tax fraud consists of an intentional violation of tax laws or regulations and is strictly forbidden. You must not directly or indirectly collaborate with clients of Euroclear to allow them to escape their fiscal responsibilities. You may not respond to requests from clients, or contact clients, in order to give tax advice, unless you have consulted a tax lawyer from Euroclear's legal division.

1.15 Report the matter immediately to your Euroclear contact point if you know or suspect that a Euroclear Company is in violation of laws, regulations or policies.

1.16 Read and comply with the relevant fact sheets including (but not limited to): data protection, competition law, anti-money laundering & counter terrorist financing and market abuse prevention. The full list of corporate policies is available on Pulse+.

2. Security Requirements

2.1 Euroclear Laptops and Teleworking

a. Only authorized laptops using authorized configurations and software are allowed to connect to Euroclear's IT network.

b. Users must not install unauthorized software or change the security settings of Euroclear software.

c. Before leaving the device unattended, the user must lock their screen.

d. Remote-access users are strongly advised to connect their laptop to the company network every week (remotely or in the office), however it is mandatory to connect locally at least once a month, to ensure that essential software is updated.

e. Users must take reasonable precautions to avoid their screen being overlooked ('shoulder surfing') by another person, when working on their corporate laptop in a public area (e.g. train).

f. Laptops must never be left unattended in public areas.

g. Users must not engage in any illegal or unethical activity while using Euroclear laptops.

h. Users must immediately report to Euroclear's Help Desk ext. 2424 (Nordics Local CT Service Desk) in case their laptop is lost or stolen.

2.2 Bring your own device

a. Euroclear grants authorized users the ability to access their corporate e-mails and calendar using their personal mobile device (for security and compatibility reasons).

b. All users must sign the End-User agreement document and comply with all its statements. Once the access has been authorized by Euroclear, the user must register his/her device(s). Please refer to 'Bring Your Own Device (BYOD) implementing Procedure' for more details.

c. The user shall remove all Euroclear data from the device on termination of employment, or withdrawal of access to the service.

d. The end-user shall ensure the following :

- A security profile is installed on the personal device to enforce a set of controls such as : mandatory use of a PIN code (at least 6 characters) to unlock the device, an automatic locking of the device if it remains inactive for 2 minutes, etc.
- The operating system (iOS version) should never be lower than the Euroclear recommended version.
- Any notifications from Euroclear's support staff must be promptly complied with.

e. The end-user must immediately report to Euroclear Help Desk ext. 2424 (Nordics Local CT Service Desk) in case their device is lost or stolen. Euroclear operators will then attempt to remotely lock & wipe Euroclear's data and, if expressly requested by the end user, the user's own data from the device.

2.3 Corporate e-mail

a. Euroclear's corporate e-mail is to be used with professional discretion and integrity.

b. Users must not open or save to disk, e-mails where the attachment is received from an unknown originator ; such e-mails are to be deleted. The end-user must alert the CIRT team (cirt@euroclear.com) if a suspicious e-mail or attachment is received and not open them.

c. Corporate, clients and third-party information cannot be sent or forwarded to private email accounts.

d. Users are not to, recklessly or deliberately propagate any malware or purposefully written malicious code, that would cause damage to Euroclear's networks/systems, or those belonging to a third party.

2.4 Internet Usage

a. Connection to the internet is only allowed through authorized and secure facilities provided by Euroclear.

b. The end-user shall be vigilant to the threat of computer malware. Anyone who suspects that malicious code has been introduced via internet activity, must immediately inform the CIRT team (cirt@euroclear.com).

c. The user are not allowed to make use of internet facilities to upload or transfer any data owned or processed by Euroclear outside of the normal conduct of business. This includes the use of internet mail, social media, video/audio hosting sites and cloud facilities such as Dropbox, Google Drive, etc.

2.5 Removable Media

a. To reduce the risk of data theft/leakage, Euroclear has disabled the USB ports on laptop devices. In exceptional circumstances, Euroclear can provide the end-user with secure encrypted USB memory sticks to be used.

b. The end-user shall immediately report if the device is lost or stolen to Euroclear Help Desk ext. 2424 (Nordics Local CT Service Desk).

c. The end-user shall return the device if no longer required.

d. The storage of sensitive data on USB memory sticks is prohibited.

2.6 Access Control and Authentication Credentials

a. The password should be easy to remember, however not obvious for everybody else (e.g. name of partner, children etc.).

b. User ID/passwords are not to be shared, at any time and under no circumstances may an employee impersonate another user.

c. Passwords must not be made known to others and should never be recorded in writing or kept in an unsecured location.

d. If anyone suspects that their password has been compromised, they should change it immediately and contact Euroclear Help Desk ext. 2424 (Nordics Local CT Service Desk).

e. Passwords should never be stored in clear text in files such as docs, scripts, macros etc.

2.7 Clear Desk Guidelines

a. The end-user shall secure documents which are of a sensitive nature when she/he is away from the desk for a long period and at the end of the day.

b. No documents must be left in meeting rooms. The meeting organizer is responsible for the removal of any remaining documents, the cleaning of the white boards and the removal of any written flip chart papers.

2.8 Physical Security

a. Do wear your Euroclear badge visibly and appropriately when in Euroclear premises at all times.

b. Always announce and escort your visitors. To announce your visitors in Brussels (visitors.brussels@euroclear.com).

c. Be aware of people who are following you closely with the purpose to gain unauthorized access to Euroclear premises (tailgating).

d. Make sure to report any kind of suspicious activity of such kind to the Security Guards (Brussels 1200).

2.9 Specific requirement for GTS and GBS admin profiles

a. The following rules are applicable to the community of personnel responsible for the development and support of corporate systems :

- All browsing must be performed from standard user accounts, never from privileged accounts.
- The user has to ensure that all downloaded software is subject to verification and malware screening before installation.
- Software shall be downloaded from legitimate vendor sites.
- The user is prohibited to access the Internet outside of defined and approved channels including directly accessing the Internet from production servers.

2.10 Security awareness and training

a. The user should have a security mindset, protect data & assets and complete all the mandatory awareness modules (security, risk, and compliance) timely.

3. Health and Safety

When on Euroclear premises

3.1 Ensure that by your actions you do not endanger yourself or others.

3.2 Conform to all local emergency procedures.

3.3 Familiarise yourself with the fire alarm system and evacuation procedures, including escape routes from the areas you frequent, and designated assembly points.

3.4 Participate in evacuation drills and follow the evacuation procedures as required.

3.5 Do not use your own personal electrical equipment on the premises without prior permission, and then only after it has had the required portable appliance testing.

Handling Equipment, Machinery and Substances

3.6 Do not move furniture or other equipment unless trained and instructed to do so.

3.7 Do not remove or alter protective equipment or other devices provided in the interest of health and safety.

3.8 Do not carry out your own repairs to plant or equipment, unless trained and instructed to do so.

3.9 Use any machinery, equipment, dangerous substance, transport equipment, means of production or safety device provided in accordance with any training and instruction given.

3.10 Where exposure to substances hazardous to health is required as part of your duties, ensure you adhere to the requirements of any control of substances hazardous to health assessments.

What to report

3.11 Report all damage and health and safety hazards to your Euroclear contact point.

3.12 Inform your Euroclear contact point of any work situation or matter which represents either a serious and immediate danger or a shortcoming in Euroclear's health and safety precautions.

3.13 Report all accidents, incidents (including "near misses"), dangerous occurrences and notifiable diseases to your Euroclear contact point, as soon as possible after the event.

3.14 Report any electrical fault with portable electrical equipment or machinery immediately. The equipment or machine should be unplugged and a suitable warning notice should be affixed to it.