

House rules of the European Central Bank for external staff

§ 1 Scope of application

1. These house rules apply to all contractors (the 'Contractors') working on the premises of the European Central Bank (ECB) as well as to their directors, agents, staff, free-lancers and subcontractors (collectively referred to as 'External staff'). The house rules form an integral part of the contract concluded between the ECB and the Contractor (the 'Contract'). In the event of a conflict, the Contract prevails.
2. ECB business areas may specify these house rules, within reasonable limits, by way of instructions to External staff working for them and may issue further guidelines and instructions on how to behave on the ECB's premises.
3. Contractors shall comply with, and ensure that their External staff comply with, these house rules and any additional guidelines and instructions issued by the ECB business area for which they are working.

§ 2 Access to ECB premises; security clearance

1. To access the ECB's premises External staff need either a personalised security badge or a visitor badge. Badges are for personal use only and are to be worn visibly at all times. In case of loss, External staff shall inform the ECB's Security Division (Extension: 069/1344-8487) thereof without undue delay.
2. External staff that have to perform duties and tasks on behalf of the Contractor at the ECB's premises, and, to this end need to move freely and unescorted on the ECB's premises, shall have a personalised security badge or an unescorted visitor badge. The issuance of such badges is subject to prior security clearance. To obtain prior security clearance, the Contractor shall provide the ECB, prior to the assignment and at the Contractor's own expense, with
 - a security self-declaration signed by the respective member of the External staff;
 - a consent form signed by the respective member of the External staff;
 - a criminal record certificate issued by the competent authority of the State of residence of the respective member of the External staff, which, in accordance with the applicable laws, lists any criminal offences for which the respective member of the External staff has been convicted or states any other adverse information (the 'Certificate of criminal record'). The Certificate of criminal record shall not be older than two months on the date it is submitted to the ECB.The ECB will provide the Contractor with the relevant forms.
3. The Contractor shall submit all security self-declarations, consent forms and certificates of criminal record in one or more separately sealed envelope(s) to the following address: European Central Bank, Security Division, Sonnemannstrasse 22, 60314 Frankfurt am Main, Germany. The envelope shall mention the words 'Security clearance' and refer to the Contract.
4. The ECB will within a reasonable time after receipt of the above-mentioned documents, conduct a security clearance check for each member of External staff in accordance with its security clearance rules and inform the Contractor about the decision taken.
5. The ECB reserves the right to refuse access to the ECB's premises to External staff for whom a security clearance check has not been conducted or for whom no security clearance has been given.
6. On the ECB's premises, access to certain offices (red dot offices) or certain areas is restricted. External staff shall not enter into such offices or areas unless explicitly authorised to do so. The access to highly secured areas (so-called security zone 5) requires a special personalised badge including biometric enrolment.

§ 3 General security rules

1. External staff shall comply with the following security rules:
 - valuable personal belongings shall not to be left unattended. Any loss or suspected theft of either ECB or personal property shall be reported to the ECB's Security Division immediately. Lost and found items shall be reported or handed in to the ECB's Security Service Centre or security staff;
 - candles and other naked flames are prohibited on the ECB's premises;
 - private electrical devices are not allowed unless External staff need them for the fulfilment of their duties;
 - animals are not to be brought into the office areas of the ECB;
 - smoking on the ECB premises is restricted to certain designated areas.
2. The ECB's Security Division may issue further guidelines and instructions to ensure security and safety on the ECB's premises. External staff shall comply with such guidelines and instructions as communicated to them.

§ 4 Emergencies

1. In case of an emergency, sudden illness, injury or accident, External staff shall call the ECB's in-house 24-hour emergency Phone number which is 111. External staff shall not place emergency calls directly to the police, the fire brigade or external medical services.
2. In case of an emergency, External staff shall follow the instructions broadcasted via the public address system and/or the instructions of ECB staff.
3. In case of a crisis situation affecting access to the ECB's premises, External staff shall call 0800/1344-1344 for further guidance.

§ 5 Use of ECB equipment

1. External staff shall use all rooms, facilities and equipment Made available by the ECB solely for the fulfilment of their duties under the Contract and handle all facilities and equipment with due care.
2. External staff are not authorised to use the ECB's parking facilities.
3. If External staff carry out technical works on the ECB's premises, they shall comply with the applicable German regulations on health and safety at work.

§ 6 Use of the ECB's IT facilities

1. If External staff are granted access to the ECB's information Technology (IT) facilities, they shall use such facilities solely for the fulfilment of their duties under the Contract and shall handle all facilities with due care.
2. When using IT facilities, External staff shall comply with the ECB's rules on information systems (IS) security and the rules on the use of IT facilities and the Internet as published on the ECB's intranet. External staff shall, in particular:
 - observe the rules on the use of their personal user identification and the secure use of their workstation and the information therein;
 - comply with the rules on the protection and regular change of assigned passwords, as well as protection of other security devices and tools (e.g. encryption keys and smart cards);
 - not abuse the IT facilities to annoy, harass, terrify, intimidate, threaten, offend, or bother any other person or conduct illegal activities;
 - not introduce, access, store, distribute or display inappropriate material or access inappropriate websites or pages containing material which could adversely affect the ECB's reputation (e.g. related to racism, pornography, violation of human rights, etc.);
 - respect the rights and property of other users and third parties and comply with relevant legal requirements

House rules of the European Central Bank for external staff

- (intellectual property, copyrights, software licences, etc.);
- not duplicate or install any software unless authorised to do so;
 - not connect any non-ECB laptop or workstation to the ECB network;
 - not use any unauthorised USB storage devices to store ECB-related data;
 - not download data from unauthorised removable media;
 - not initiate any actions that may be interpreted as legally committing the ECB to third parties such as ordering goods and services via e-mail, joining chain letters or accepting 'get rich quick' offers;
 - not open any suspicious e-mails or download any software or documents from the Internet unless explicitly requested by ECB staff;
 - not forward their ECB internal mail automatically to other external mailboxes. Manual forwarding is subject to the confidentiality rules;
 - not publish detailed information about their tasks or responsibilities at the ECB and refrain from making statements about their personal opinions or beliefs which may be perceived as statements representing the ECB on websites which are accessible to the general public, including private homepages or social network sites;
 - use their ECB e-mail account (if any) for any ECB business communication. Other Internet tools, such as instant messaging portals, shall not be used;
 - not exchange or store ECB-related information via unauthorised Internet storage services.
3. If in exceptional cases External staff are entrusted with an ECB laptop, they are personally responsible for its physical and technical security at all times. To protect the laptop, External staff shall comply with the following rules:
- a carry case shall be used during travel to minimise damage to hardware during transport. The laptop shall not be left unattended;
 - the laptop shall be locked using a physical lock or stored in a locked cabinet when not in use;
 - the attached identification labels shall not be removed;
 - the screen shall be locked or the currently logged-on user needs to be logged off when the laptop is not in active use; External staff shall verify that the screensaver is functioning properly;
 - External staff shall protect themselves against the risk of shoulder surfing and use a screen filter which can be ordered from the ECB;
 - passwords used on laptops shall comply with the ECB's policy on passwords. Passwords shall never be written down and stored with the laptop;
 - transfer of data from the laptop to another PC should be executed using the encrypted USB stick provided by the ECB;
 - when using a network connection outside the ECB, External staff shall minimise risk exposure by (i) closing all other connections to other networks when using the laptop to access the ECB network remotely and (ii) whenever possible, use Ethernet cable connections instead of wireless connections. Encrypted WPA2 wireless connections shall be used when no cable alternative is available;
 - the laptop shall be brought back to the ECB and connected to the ECB LAN every month, or when requested by the IS Service Desk, in order to implement security updates. This opportunity shall be taken to save all documents created or updated offline on the laptop;
 - installation and set-up of the laptop may not be changed.
4. External staff shall promptly report any incident related to the use of IT facilities to the ECB business area for which they are working or the IS Service Desk (Extension: 069/1344-7777). They shall not seek to conceal such actions or to rectify such incidents themselves.

§ 7 Use of telephones and fax equipment

If External staff have an office work place on the ECB's premises, they may use the ECB's telephone facilities and the fax equipment for the fulfilment of their duties under their Contract. The use of such facilities for other purposes is prohibited unless the External staff use a personal, pre-paid telephone account. For private purposes, External staff may use the public phones available on the ECB's premises.

§ 8 Storage of documents; confidentiality

1. External staff shall store and record any information, data or documents in accordance with the instructions given to them by ECB staff.
2. External staff shall treat in strictest confidence and not divulge to unauthorised persons any information, data or documents concerning the ECB, its staff, the Contract or its performance, which the ECB designated orally or in writing as 'ECB-Restricted', 'ECB-Confidential', or 'ECB-Secret' or which a reasonable contractor would consider to be confidential (the 'Confidential information'). External staff shall only use such Confidential information for the purpose for which it was disclosed and shall not use or exploit such Confidential information for their own benefit or for the benefit of any other person.
3. External staff shall not reply to requests from the media or other external parties and shall forward any request for information or documentation to the ECB business area for which they are working.
4. External staff shall store documents classified as Confidential information in locked cabinets or containers.
5. External staff shall not take Confidential information outside the ECB's premises and shall not forward such Confidential information by e-mail, fax or any other means to any external party unless explicitly authorised to do so. If, exceptionally, External staff are authorised to take Confidential information outside the ECB, they shall take all reasonable measures to ensure that unauthorised persons do not obtain access to such documents.
6. External staff shall dispose of Confidential information only in the confidential waste containers available on each floor.

§ 9 Leaving the ECB

1. If External staff leave the ECB or work for another ECB Business area, they shall inform their contact person at the ECB in good time before their last day so that electronic data (files on the users' local and network drives and e-mail folders, etc.) can be preserved to the extent needed by the business area.
2. External staff shall return all items received from the ECB, including their security badge, keys, books and IT equipment, if any.