EUI EUROPEAN UNIVERSITY INSTITUTE

EUI Contractors' Policy

Version 1.0 – Short version for the publication

Contents

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Document Information

Title**: EUI Contractors' Policy**	Author: **Laura Biagiotti**
Classification: **PUBLIC**	Area: **EUI IT Security**
Version: 2**.0**	Version Date: 27/10/2020

Document Control

	Version	Name	Date	Comments
Developed by:	1.0	Laura Biagiotti	27/10/2020	

	Version	Name	Role	Date	Comments
Reviewed by:	1.0	Laura Biagiotti	DSO	02/08/2022	Short form for the public release

	Version	Name	Role	Date	Comments
Approved by:	1.0	David Scott	ICT Director	27/10/2020	

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

1. Scope

1.1 This policy applies to all Contractors and persons employed by Contractors carrying out a processing operation governed by a contract, or another binding legal act stipulated in writing.

1.2 This policy is also mentioned in the Identity Access Management Policy (IAM Policy) relating to Identities of external contractors and collaborators (point 6).

1.3 This policy, also, indicates the activities not permitted at the EUI.

2. Definitions

A "*Contractor*" is a natural or legal person that process personal data for the EUI or on behalf of the EUI's Controller.

3. Responsibilities

3.1 The Contractor shall communicate to the Unit the list of persons that carrying out the service at the EUI or require access to EUI systems to provide the service.

3.2 The Contractor shall promptly communicate any changes to the persons employed that may have an impact on the service provided such as a change of function or dismissal.

3.3 The Contractor shall ensure that their employees follow organisational and security policies[1] published under Policies in the ICT Service website including the "*EUI Acceptable Use Policy*", the "*Consequences of Misuse and Hacking of IT resources: Policy*" and *GARR Acceptable Use Policy*.

3.4 The Contractor shall inform its employees on how to report a data breach.

3.5 The Data Controller - DC (or the Delegated Data controller - DCC) of the Service or academic Unit is the one that can authorise the access requested for the purposes of ensuring compliance with the EUI Data Protection Policy (President Decision nº 10/2019).

[1] The security policies are published on the ICT Service website at the following link: https://www.eui.eu/ServicesAndAdmin/ComputingService/Security.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

3.6 According to the Article 22 of EUI Data Protection Policy[2], the detailed list of obligations for those performing external processing of personal data on behalf of Controllers is provided.

4. Confidentiality clause[3]

4.1 The EUI and the Contractor shall treat with confidentiality any information and documents, in any form, disclosed in writing or orally in relation to the performance of the contract (or Framework contract) and identified in writing as confidential.

4.2 The Contractor shall:

a. not use confidential information and documentation for any purpose other than fulfilling its obligations under the contract (or Framework contract) without prior written agreement of the EUI;
b. ensure the protection of such confidential information and documentation with the same level of protection it uses to protect its own confidential information, but in no case any less than reasonable care;
c. not disclose directly or indirectly confidential information and documentation to third parties without prior written agreement of the EUI.

4.3 The confidentiality obligation set out in Article 4.1 shall be binding on the EUI and the Contractor unless:

a. the disclosing party agrees to release the other party from the confidentiality obligation earlier;
b. the confidential information becomes public through other means than via breach of the confidentiality obligations, through disclosure by the party bound by that obligation;
c. the disclosure of the confidential information is required by law.

4.4 The Contractor shall obtain from any person with the power to represent it or take decisions on its behalf, as well as from third parties involved in the performance of the contract (or

[2] EUI Data Protection Policy, extract of Article 22 titled "*External processing of personal data on behalf of Controllers*" "*1. The carrying out of a processing operation by an external Processor shall be governed by a contract or another binding legal act (see Annex I to this Decision) stipulating in writing that the Processor: a) processes the data only on instructions from the Controller; …*".

[3] The Confidentiality clause is subscribed by Contractors in the Framework contracts or Contract with the EUI.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Framework contract), an undertaking that they will comply with the confidentiality obligations set out in Article 4.1.

5. Duties of the persons employed by Contractors

5.1 The persons employed by Contractors may carry out personal data processing operations, provide consulting service getting the knowledge of EUI infrastructure, system and network and have privileged access to systems, network, application and website;

5.2 The persons employed by Contractors are required to subscribe the Declaration of Confidentiality (see template in Appendix 1) in compliance with the EUI Data Protection Policy (PRESIDENT DECISION No. 10/2019 of 18 February 2019) and in order to ensure strict confidentiality and not disclose directly or indirectly confidential data, information, knowledge and documentation to third parties without prior written agreement of the EUI;

5.3 The subscription of the Declaration of Confidentiality is required before providing the EUI credentials (login and password) and email address;

5.4 The subscription of the Declaration of Confidentiality should be updated when there is a significant change or an addition in the field of operations.

6. Obligations for the persons employed by Contractors - Activities not permitted at the EUI

6.1 The following activities are not permitted at the EUI to Contractors (including self-employed) and persons employed by Contractors:

i. the use of hacking tools;
ii. the use of anonymisers;
iii. to share (or disclose) the individually assigned EUI credentials (login and password) to another person or third parties;
iv. the collection of logs from systems, applications and websites;
v. using network, storage or computing services or resources, connecting hardware or services or software to the network, disseminating viruses, hoaxes, or other programs in such a manner that the activities of other persons, users, or services which are available within the EUI infrastructure and network may be harmed, or disrupted;

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

vi. creating or transmitting or store any images, data, or other material, which may be offensive, defamatory, obscene, or indecent, or which may offend human dignity, especially if pertain to gender, race, or religious beliefs;

vii. the use of EUI resources for commercial or private use including non-profit, gambling, mining cryptocurrencies and hosting third parties services;

viii. performing scan, vulnerability assessment and penetration testing is not permitted at the EUI unless explicitly authorised in writing by the Controller and Data Security Officer.

7. Processing of personal data[4]

7.1 Where the contract (or framework contract) requires the processing of personal data by the Contractor or any of its subcontractors, the Contractor may act only under the supervision of the data controller, in particular with regard to the purposes of the processing, the categories of data which may be processed, the recipients of the data and the means by which the data subject may exercise its rights. In that respect, the contractor shall be bound by the relevant provisions of the EUI's President's Decision No. 10/2019 of 18 February 2019 as well as by the General Data Protection Regulation (GDPR) /Regulation (EU) 2018/1725 and Regulation (EU) 2016/679 and all applicable nationals laws and regulations of the country where it is established regarding to the processing of personal data and privacy.

7.2 The Contractor shall grant its personnel access to the data only to the extent strictly necessary for the performance, management and monitoring of the contract (or framework contract).

7.3 The Contractor undertakes to adopt appropriate technical and organisational security measures having regard to the risks inherent in the processing and to the nature of the personal data concerned in order to:

a. prevent any unauthorised person from gaining access to computer systems processing personal data, and especially:

i. unauthorised reading, copying, alteration or removal of storage media;

[4] This clause is subscribed by Contractors in the Framework contracts or Contract with the EUI.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

ii. unauthorised data input, as well as any unauthorised disclosure, alteration or erasure of stored personal data;

iii. unauthorised use of data-processing systems by means of data transmission facilities;

b. ensure that authorised users of a data-processing system can access only the personal data to which their access right refers;

c. record which personal data has been communicated, when and to whom;

d. ensure that personal data being processed on behalf of third parties can be processed only in the manner prescribed by the EUI;

e. ensure that, during communication of personal data and transport of storage media, the data cannot be read, copied or erased without authorisation;

f. design its organisational structure in such a way that it meets data protection requirements.

8. Security of processing

8.1 According to the EUI Data Protection policy art. 21 par 2 (d), "the Controller determines the purpose and means of the processing of personal data implementing appropriate technical and organisational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data processed. Such measures shall be taken to prevent any personal data breach. Controllers give the Processors instructions for the notification of security breaches, in accordance with Article 13 of this Decision";

8.2 The Controller undertakes to adopt appropriate technical and organisational security measures including but not limited to:

a. the subscription of Declaration of Confidentiality to the persons employed by contractors as detailed in paragraph 4 above;

b. the publication and dissemination of information concerning organisational and security policies[5] published under Policies in the ICT Service website including the "EUI

[5] The security policies are published on the ICT Service website at the following link: https://www.eui.eu/ServicesAndAdmin/ComputingService/Security.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Acceptable Use Policy", the "Consequences of Misuse and Hacking of IT resources: Policy" and GARR Acceptable Use Policy;

c. provide Cyber security awareness training to persons employed by Contractors when deemed necessary for the data processing performed;
d. communicate on how to report data breach
e. perform Security logging as detailed in art 9.

9. Security logging

The activities performed on EUI network, systems, applications and websites may be registered in various logs for security purposes. The "*ICT5 Security monitoring on digital systems*", (Notification form and Privacy statement) provides a detailed description of security logging; it is part of the EUI Data Registry under ICT Service published on EUI Data Protection website available at: https://www.eui.eu/About/DataProtection.

10. Document Owner and Approval

The ICT service is the owner of this document and is responsible for ensuring that this procedure is reviewed every year or upon significant changes of technology and regulation. A current version of this document is available and published on the EUI ICT Service website. This policy was approved by DC and DDC of ICT Service on 27/10/2020 after receiving a positive opinion of DPO.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Appendix 1- Declaration of confidentiality (sample)

Non-Disclosure agreement

Declaration of confidentiality

(*to be subscribed by an employee of an external company*)

The undersigned, [Name SURNAME], ID card number _____ issued by _____ on _____ employee of [insert the name of the company] acting as an external collaborator of the EUI on behalf of the abovementioned company in the field of (e.g. User support, Network services, telephony, Windows/Linux system administration, information security, email configuration..), expressly declares that he/she will hold all details, data, information and knowledge to which he/she has access through the exercise of that role in strict confidence.

Both during and after completion of the tasks related to (list of assignments or project name) the undersigned will exercise and ensure strict confidentiality with respect to third parties and shall not copy these details, data, information and knowledge.

He/She will also fully respect any obligations related to the protection of personal data as provided for by the applicable rules of the EUI Data Protection Policy (PRESIDENT DECISION No. 10/2019 of 18 February 2019). Mr/Ms XX has received a copy of the EUI Data Protection Policy. He/She will also fully respect the organisational and security policies[6] published in the ICT Service website including:

- EUI Acceptable Use Policy
- Consequences of Misuse and Hacking of IT resources: Policy

Date ...../...../.....

Signature

---

[6] The security policies are published on the ICT Service website at the following link: https://www.eui.eu/ServicesAndAdmin/ComputingService/Security.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Appendix 2 - External Account Registration Form (sample)

External User Registration Form

This form should be used by external collaborator or employee of contractor to provide personal details. Information collected will be used to generate credentials granting access to EUI resources.

Name:	
Surname:	
Date of Birth:	
Place of Birth (Country):	
Gender: (M/F/X)	
Company e-Mail address: (not EUI e-Mail)	
Company name	
Unit/Department: (INTERNAL USE ONLY)	
Start date / End date (1)	

(1) End date: please note that for multiple years contract, the maximum allowed period of validity is one year, renewable.

I, _____, declare the following statement

☐ I **give** consent to process my data in accordance with the EUI Data Protection Policy.

☐ I **do not give** consent to process my data in accordance with the EUI Data Protection Policy (The refusal precludes the Institute from processing your data and granting both physical and IT access to services managed by EUI).

Date: __ / __/ __ Signature: _____

INTERNAL USE ONLY – External user needs:

☐ Computer Access ☐ EUI e-mail address ☐ EUI ID Card

EUI Identity manager of the Unit:

The form is compliant with the Decision of the President No. 10 of 18 February 2019 (EUI Data Protection Policy). Please refer to the IAMS Privacy Statement for details on data processing and the Contractors' policy

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu

Appendix 3 - Consequences of Misuse and Hacking of IT resources: Policy

EUI users, Contractors and person employed by Contractors and guests infringing the above rules and regulations face sanctions which may vary from temporary suspension to termination of service(s) or of the personal computing account itself. In the event of significant or repeated violation of the present guidelines, the Director of the ICT Service will lodge a complaint to the disciplinary Committee of the EUI according to the Disciplinary Regulations. Because of its potentially serious consequences for the work and well-being of the Institute, hacking will be generally regarded as gross misconduct.

Where hacking is a criminal offence, offenders may also be liable for criminal prosecution. Violation of copyright held by individuals and corporations or other entities can result in civil and criminal liability on the part of the infringer. Also, distribution of Internet viruses, worms, and Trojan horses can lead to civil and/or criminal liability.

Tel. [+39] 055 4685 590
Fax. [+39] 055 4685 205
compserv@eui.eu

Villa il Poggiolo, Piazza Edison 11,
50133 Firenze (FI), Italy
www.eui.eu