LOG MANAGEMENT POLICY

Approval
Date: **15/09/2021**
ASI Manager: **Dr Francesca Pruneti**
Digitally signed pursuant to Legislative Decree No. 82/2005

Automatically translated by DeepL

About the document		
Edited by: *O.U. IT Security*	**Target audience:** *IT system operators providing services to users of the University of Parma*	**Document deposit:***www.unipr.it/regolamento- security-EN*

Summary

1. Purpose of the document

The purpose of this document is to define the types of logs to be kept and the retention rules to be applied, in particular highlighting which information must be tracked and for how long.

2. Scope of application

The policy described in this document applies to the logs of IT systems that provide services to users of the University of Parma.

3. Need for log retention

The management of logs by the University is necessary to ensure compliance with the legislation protecting personal data, as it allows the reconstruction of the activity of an IT system and the identification of possible liability in the event of errors, violations of the law and databreach (Art. 33 paragraph 3 of EU Regulation 2016/679). The principle of accountability (Art. 5 para. 2 of the EU Regulation 2016/679) introduces for the first time, the obligation for the data controller to demonstrate compliance with the legislation by deciding autonomously on the modalities, guarantees and limits of the processing of personal data, in consideration of the operational context in which one finds oneself. On the one hand, therefore, data controllers not only have to carry out all necessary activities to safeguard data subjects, but they also have to provide proof of compliance in the event of inspections by the competent authorities.

4. Log persistence

Logs must be stored and maintained appropriately to prevent any loss of information or possible compromise by intruders. Log retention must also comply with regulatory requirements and provide the necessary information for forensic and incident response activities.

5. Log correlation

The logs must be managed centrally and accessible to the IT Security O.U. in order to be able to carry out automated correlation of the information they contain. in order to meet regulatory requirements and provide sufficient information necessary for forensic, incident response and databreach analysis activities.

6. Implementation Status

The logs currently being tracked are those of the green-coloured lines

Tracking data at the application level (highlighted in the table below in brown colour), should be stored in accordance with regulatory provisions, applying encryption, anonymisation, minimising retention times and giving adequate information to those concerned in compliance with legal provisions and trade union agreements; therefore, they can only be implemented after all the above steps have been taken.

7. Log table

Categories and types	What to track	Systems interests you	Time of preservation	Reference Standards	Description
System administrator access and privileged profiles	• Username • Timestamp • Event description: Log-in, Log-out, Attempts failed • Accessed processing system	• Operating Systems • Complex software • Network equipment	Min 6 months Max 2 years	1. Measures and precautions prescribed for the holders of processing operations carried out electronic means with regard to the attribution system administrator functions - 27 November 2008 Official Journal No. 300 of 24/12/2008 2. Minimum ICT Security Measures for Public Administrations, 26 April 2016	1. *"... the recording events generated by the computer authentication system upon access or attempted access by a system administrator or upon disconnection of the system administrator in the context of interactive connections to processing systems or to software systems..."* (Log-in, log-out and failed attempts) 2. 5.5.1 failed login attempts with an administrative user in the logs. N.B. System Administrators must not have access to these logs, which must be non-modifiable
Changes to administrative utilities	• Adding users with administrative privileges • Deleting users with privileges administrative	• Operating Systems • Complex software • Network equipment	Min 1 year Max 2 years	Minimum ICT Security Measures for Public Administrations, 26 April 2016	*5.4.1 Tracing the addition or deletion of a user administrative.*
Activities of system administrators and privileged profiles	• Username • Timestamp • Operations performed	• Operating Systems • Complex software	Min 1 month Max. 6 months	1. ISO 27001 2. Minimum ICT Security Measures for Public Administrations	1. 12.4.3 The activities administrators and operators must be logged, and they must

	• Accessed processing system			Administration, 26 April 2016	be protected and reviewed periodically. 2. 5.1.4 Record the actions performed by an administrative user and detect any abnormal behaviour.
Authentication and Single Sign On for all web services federated with the system of authentication of the Athenaeum	• Timestamp • Username • Log-in, • Log-out • Service • IP	Server of authentication ne (LDAP, AD, Radius, Shibboleth, CAS etc.)	Min 1 month Max. 1 year	1. Work: the Garante's guidelines for e-mail and internet Official Journal No. 58 of 10 March 2007 2. CODAU Guidelines on Privacy and Data Protection in Universities	1. *"...the use of the Internet by workers may in fact be subject to analysis, profiling and full reconstruction by processing log files of web surfing obtained, for example, from a proxy server or other information logging tool..."* 2. *"System and network tracking This includes tracking data generated by network equipment and components infrastructure."*
Navigation web (can be activated incidents and on specific sub-sets)	• Source IP • Destination IP • Source port • Destination port • Protocol • URL visited	Equipment manages access to the Internet (e.g. Firewall, IPS, etc.).	Depending on of the purpose to be pursued	Labour: the guidelines of the Garante by post electronics and the internet Official Gazette No. 58 of 10 March 2007	"...the use of the Internet by part of the workers can in fact form the subject of analysis, profiling and full reconstruction by processing log files of navigation web obtained, for example, by a proxy server or a other instrument of registration of information...'
DHCP server operations	• Macaddress-IP Association • Association user-mac	Automatic release systems	Min 1 year Max 2 years	1. Minimum ICT security measures for public authorities	*1.2.1 Implement the "logging of operations of the DHCP server.*

	address (stored separately from the previous association)	of IP addresses		Administration, 26 April 2016 2. Responding to a request from the competent administrative supervisory, inspection or judicial authorities	
WIFI Access	• User ID • IP address and MAC address • AP Name • Timestamp (start and end of session) • Type and OS version • Number of bytes exchanged	WIFI access systems	Min 1 year Max 2 years	Responding to a request from the competent administrative supervisory, inspection or judicial authorities	
VPN Access	• User ID (with any network access roles) • IP address (both external and internal) • Timestamp	VPN concentrators	Min 1 year Max 2 years	Responding to a request from the competent administrative supervisory, inspection or judicial authorities	
Firewall events, IPS and other network equipment	Activate firewall IPS modules	Control and network equipment	Min 15 days Max. 6 months	1. Minimum ICT Security Measures for Public Administrations 26 April 2016 (standard classification) 2. ISO 27001	1. *8.1.3 Events detected by the instruments are sent to a central repository (syslog) where they are permanently stored.* 2. *13.1.1 Appropriate logging and monitoring activities should be applied to record and detect actions that could have an impact on information security*

User activity on file repositories	• Timestamp • Username • Hostname • Access to files • File creation • File deletion • File editing	Centralised repositories of University data (e.g.: File server, SharePoint etc.)	Min 15 days Max. 6 months	1. ISO 27001 2. EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34) 3. Minimum ICT Security Measures for Public Administrations, 26 April 2016	*1. 12.4.1 Event logs recording user activities, exceptions, failures and information security events should be produced, maintained and regularly reviewed.*
Use and management of workstations	• Timestamp • Log-in, • Log-out • Username • Hostname • IP • Inventory of the hardware and software installed/used	• PDL • VDI	Min 6 months Max. 1 year	1. EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34) 2. Minimum ICT Security Measures for Public Administrations, 26 April 2016 3. Responding to a request from the competent administrative supervisory, inspection or judicial authorities	
Access to computer laboratory workstations	• Timestamp • Log-in, • Log-out • Username • Hostname • IP	Physical and virtual classrooms	Min 6 months Max. 1 year	1. EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34) 2. Minimum ICT Security Measures for Public Administrations, 26 April 2016 3. Responding to a request from the competent administrative supervisory, inspection or judicial authorities	
Management of telephone traffic for the purposes of	Call data in/out (not content and numbers partly with asterisks)	Traditional and VOIP telephony systems	Min 1 month Max. 6 months	EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34)	

accounting					
Applications for requests for action	• User master data • Ticket reason	Ticket Management Systems	Min 1 year later the data is anonymised	EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34)	
Printing Services	• Timestamp • Username • Hostname	Centralised printing systems	Min 1 year later the data is anonymised	EU Regulation 2016/679 (Art. 5, Art. 33 and Art. 34)	
Accident Register	• Accident type • Vehicle • n. impacted • no. damaged • source report • notes • Actions of containment and restoration • Reopenings case • Responsible activities malevolent • Databreach • Notification guarantor • Notification interested		Min 2 years later the data is anonymised	Responding to a request from the competent administrative supervisory, inspection or judicial authorities	

Document Revisions

Ver.	Description of changes	Author	Date modification
1.0	*Initial version*	*O.U. IT Security*	*02/07/2020*