# NETWORK TRAFFIC FILTERING POLICY

| Approval |
| --- |
| Date: **01/09/2023** |
| ASI Manager: **Dr Francesca Pruneti** |
| Digitally signed pursuant to Legislative Decree No. 82/2005 |

| About the document | | |
| --- | --- | --- |
| **Edited by:**<br>*O.U. IT Security*<br>*O.U. Technology Systems and Infrastructure* | **Target audience:**<br>*Anyone using data, services and IT resources of the University of Parma* | **Document deposit:***www.unipr.it/regolamento- security-EN* |

Automatically translated by DeepL

## Summary

## 1. Purpose of the document

The purpose of this document is to define a policy for filtering data, services and IT resources owned by the University of Parma, with the aim of increasing IT security and protecting privacy.

## 2. Scope of application

The policy described in this document applies to data exchanges that occur between the University of Parma networks, devices, applications, services towards the Internet and between them, on the internal network or in the cloud. Any data flow originating or arriving at University of Parma IT resources, whether internal or cloud, is potentially subject to the filtering policies described in this document.

## 3. Cloud network data flow filters

E-mails are filtered according to the probability of being SPAM. Automated analyses define the 'reputation' level of messages based on various elements; if the 'reputation' level is not appropriate, the message is considered SPAM and placed in the 'Junk Mail' folder instead the 'Inbox' within the user's mailbox.

E-mail messages and collaboration programmes made available by the University undergo rewriting of the web links contained within them. Thus, if the user clicks on a link that has been categorised as malicious, he is blocked from accessing the dangerous web resource.

Similarly, documents attached to e-mail messages, or shared through collaboration programmes, are scanned before they are made available to the user or after they are made available (provided they are in the cloud disk space). If the documents are deemed malicious, they are deleted or otherwise made inaccessible to the user.

The forwarding of University e-mails to personal (non-UNIPR) mailboxes is blocked, as messages forwarded to other mail handlers are not subjected to the IT security controls set up by the University (the forwarding block has been in place since 30 October 2022 following the 'Rector's note on e-mail security' sent to the University's structured personnel on 26 October 2022).

## 4. Filters on internal network data flows

Data traffic entering and leaving the University's internal network is filtered to prevent access to resources that may carry malware (e.g.: Ransomware, Botnets, DarkWeb, anonymous VPNs, SPAM URLs, etc.), illegal or inappropriate material (e.g.: illicit substances, pornography, extremism, abuse, etc.), copyrighted material. Traffic is filtered on the basis of pre-defined categories and databases of known malicious resources.

Filters are applied for traffic from both the physical (wired) and wireless (WiFi) network infrastructure.

Below is the table of filtered content categories and their perimeter actions.

| Categories | Actions |
|---|---|
| **Adult/mature Content** | |
| Abortion | Allow |
| Advocacy Organisations | Allow |

| | |
|---|---|
| Alcohol | Allow |
| Alternative Beliefs | Allow |
| Dating | Allow |
| Gambling | Allow |
| Lingerie and Swimsuit | Allow |
| Marijuana | Allow |
| Nudity and Risque | Allow |
| Other Adult Materials | Allow |
| Pornography | Block |
| Sex Education | Allow |
| Sports Hunting and War Games | Allow |
| Tobacco | Allow |
| Weapons (Sales) | Allow |
| | |
| **Bandwidth Consuming** | |
| File Sharing and Storage | Allow |
| Freeware and Software Downloads | Allow |
| Internet Radio and TV | Allow |
| Internet Telephony | Allow |
| Peer-to-peer File Sharing | Block |
| Streaming Media and Downloads | Allow |
| | |
| **Potentially Liable** | |
| Child Abuse | Block |
| Discrimination | Allow |
| Drug Abuse | Allow |
| Explicit Violence | Block |
| Extremist Groups | Block |
| Hacking | Allow |
| Illegal or Unethical | Allow |
| Plagiarism | Allow |
| Proxy Avoidance | Block |
| | |
| **Security Risk** | |
| Dynamic DNS | Block |
| Malicious Websites | Block |
| Newly Observed Domain | Warning |
| Newly Registered Domain | Warning |
| Phishing | Block |
| Spam URLs | Block |
| **Unrated** | Warning |

Allow: action permitted

Block: action denied

Warning: the user is warned, but may decide to continue

## Document Revisions

| Ver. | Description of changes | Author | Date modification |
|---|---|---|---|
| *1.0* | *Initial version* | *U.O. Technological Systems and Infrastructure* | *01/09/2021* |
| *1.1* | *Added mail forwarding block* | *O.U. IT Security* | *25/01/2023* |
| *2.0* | *Filter division between cloud and internal networks* | *O.U. IT Security* | *25/08/2023* |