EUROPEAN
COMMISSION

Brussels, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

ANNEXES

to the

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union

{SWD(2022) 67 final} - {SWD(2022) 68 final}

ANNEX I

The following domains shall be addressed in the cybersecurity baseline:

(1) cybersecurity policy, including objectives and priorities for security of network and information systems, in particular regarding the use of cloud computing services (within the meaning of Article 4(19) of Directive [proposal NIS 2]) and technical arrangements to enable teleworking;

(2) organisation of cybersecurity, including definition of roles and responsibilities;

(3) asset management, including IT asset inventory and IT network cartography;

(4) access control;

(5) operations security;

(6) communications security;

(7) system acquisition, development and maintenance;

(8) supplier relationships;

(9) incident management, including approaches to improve the preparedness, response to and recovery from incidents and cooperation with CERT-EU, such as the maintenance of security monitoring and logging;

(10) business continuity management and crisis management; and

(11) cybersecurity education, awareness-raising and training programmes.

ANNEX II

Union institutions, bodies and agencies shall address at least the following specific cybersecurity measures in the implementation of the cybersecurity baseline and in their cybersecurity plans, in line with the guidance documents and recommendations from the IICB:

(1) concrete steps for moving towards Zero Trust Architecture (meaning a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries);

(2) the adoption of multifactor authentication as a norm across network and information systems;

(3) the establishment of software supply chain security through criteria for secure software development and evaluation;

(4) the enhancement of procurement rules to facilitate a high common level of cybersecurity through:

  (a) the removal of contractual barriers that limit information sharing from IT service providers about incidents, vulnerabilities and cyber threats with CERT-EU;

  (b) the contractual obligation to report incidents, vulnerabilities and cyber threats as well as to have appropriate incidents response and monitoring in place.