COMMISSIONE
EUROPEA

Bruxelles, 22.3.2022
COM(2022) 122 final

ANNEXES 1 to 2

# ALLEGATI

**della**

**Proposta di REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO**

**che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione**

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

# ALLEGATO I

Nella base di riferimento per la cibersicurezza vengono considerati i seguenti settori:

(1) la politica in materia di cibersicurezza, compresi gli obiettivi e le priorità per la sicurezza dei sistemi informatici e di rete, in particolare per quanto riguarda l'uso di servizi di cloud computing (ai sensi dell'articolo 4, punto 19, della direttiva [proposta NIS 2]) e le modalità tecniche per consentire il telelavoro;

(2) l'organizzazione della cibersicurezza, compresa la definizione di ruoli e responsabilità;

(3) la gestione delle risorse, compresi l'inventario delle risorse informatiche e la cartografia della rete informatica;

(4) il controllo dell'accesso;

(5) la sicurezza delle operazioni;

(6) la sicurezza delle comunicazioni;

(7) l'acquisizione, lo sviluppo e la manutenzione dei sistemi;

(8) le relazioni con i fornitori;

(9) il trattamento degli incidenti, compresi gli approcci per migliorare la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi e la cooperazione con il CERT-UE, ad esempio mantenendo il monitoraggio della sicurezza e le pratiche di registrazione;

(10) la gestione della continuità operativa e la gestione delle crisi, e

(11) programmi di educazione, sensibilizzazione e formazione in materia di cibersicurezza.

## ALLEGATO II

Nell'attuazione della base di riferimento per la cibersicurezza e nei loro piani di cibersicurezza le istituzioni, gli organi e le agenzie dell'Unione considerano almeno le seguenti specifiche misure di cibersicurezza, in linea con i documenti di orientamento e le raccomandazioni dell'IICB:

(1) misure concrete per passare ad un'architettura zero trust (ovvero un modello di sicurezza, una serie di principi di progettazione di sistemi, e una strategia coordinata di cibersicurezza e di gestione dei sistemi, basati sul riconoscimento dell'esistenza di minacce sia all'interno che all'esterno dei confini di rete tradizionali);

(2) l'adozione dell'autenticazione a più fattori come norma in tutti i sistemi informatici e di rete;

(3) l'introduzione di una catena di approvvigionamento del software sicura, attraverso criteri di sviluppo e valutazione sicuri del software, e

(4) il rafforzamento delle norme relative agli appalti, per facilitare il conseguimento di un livello comune elevato di cibersicurezza attraverso:

   (a) l'eliminazione degli ostacoli contrattuali che limitano la condivisione delle informazioni sugli incidenti, le vulnerabilità e le minacce informatiche fra i prestatori di servizi informatici e il CERT-UE, e

   (b) l'obbligo contrattuale di segnalare gli incidenti, le vulnerabilità e le minacce informatiche, così come di avere predisposte adeguate misure di monitoraggio e risposta in caso di incidenti.