Allegato 1

Misure di sicurezza tecniche ed organizzative

Al fine di proteggere i dati personali trattati AEIT ha adottato idonei mezzi tecnici per proteggere le comunicazioni fra le macchine, per evitare accessi non autorizzati e per limitare le probabilità e le conseguenze di danneggiamenti accidentali dell'archivio.

1. Comunicazioni client-server e server-server

I server **www.aeit.it, ammi.aeit.it, convegni.aeit.it, corsi.aeit.it, energiaelettrica.aeit.it** sono stati configurati in modo da operare esclusivamente secondo il protocollo "**HyperText Transfer Protocol over Secure Socket Layer**" (conosciuto anche come "HTTPS" o "HTTP over TLS").

Tutte le comunicazioni client-server e/o server-server hanno luogo in modalità criptata con cifratura mediante chiave a 128 bit (TLS_ECHDE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2).

I certificati SSL/TLS dei server sono stati emessi da "Let's Encrypt", Autorità certificativa riconosciuta dai browser più diffusi.

L'uso di comunicazioni in modalità criptata protegge il contenuto delle comunicazioni da tentativi di intercettazione non autorizzati che potrebbero aver luogo quando un interessato o un operatore autorizzato si collega al server utilizzando infrastrutture di rete pubbliche (sia "cablate" sia "wireless").

2. Accessi non autorizzati all'archivio

i server **www.aeit.it**, **ammi.aeit.it, corsi.aeit.it** conservano i dati personali dei Soci e dei titolari di account di tipo "Guest" mediante un archivio costituito da database gestiti dal server "MariaDB". Gli operatori autorizzati di AEIT, i Soci ed i titolari di account di tipo "Guest" non possono accedere direttamente ai database, ma possono leggere e/o modificare il contenuto dell'archivio esclusivamente attraverso un programma di gestione (un cosiddetto "CMS" o "Contents Management System") che ha il compito di proteggere i dati dell'archivio da accessi ed azioni non autorizzate.

Ogni Socio, ogni titolare di un account di tipo "Guest" ed ogni operatore autorizzato è dotato di una coppia di credenziali (username e password) con le quali deve eseguire una procedura di autenticazione ("log-in") prima di poter accedere a dati personali tramite il CMS.

Ogni Socio ed ogni titolare di account di tipo "Guest" viene ovviamente autorizzato dal CMS ad accedere esclusivamente ai propri dati presenti nella porzione di archivio conservata nei server www.aeit.it, convegni.aeit.it e corsi.aeit.it

Gli operatori autorizzati di AEIT, sempre attraverso il CMS, possono accedere ai dati presenti nella porzione di archivio conservata nel server ammi.aeit.it.

I CMS dei server www.aeit.it, ammi.aeit.it, corsi.aeit.it hanno procedure automatiche per mantenere "allineati" i rispettivi database.

Le credenziali di accesso ai server www.aeit.it, convegni.aeit.it e corsi.aeit.it (username e password) possono essere modificate dal titolare dell'account (i titolari di account di tipo “Guest” hanno username coincidente con la propria email e possono modificare solo la password). Le credenziali vengono criptate con un processo non reversibile per proteggere la privacy del titolare dell'account.

Le credenziali di accesso al server ammi.aeit.it (username e password) hanno caratteristiche di maggiore protezione data la maggiore importanza del server. Esse devono avere lunghezza compresa fra 8 e 16 caratteri, devono contenere almeno due lettere maiuscole, almeno due lettere minuscole, almeno due cifre numeriche ed almeno un carattere speciale. Le credenziali possono essere modificate dal titolare dell'account, vengono criptate con un processo non reversibile per proteggere la privacy del titolare dell'account e scadono ogni tre mesi.

I server www.aeit.it, ammi.aeit.it, convegni.aeit.it, corsi.aeit.it, energiaelettrica.aeit.it si trovano nei locali dell'Ufficio centrale AEIT, in via Mauro Macchi 32 a Milano. In base alla terminologia usata nel GDPR l'Ufficio centrale AEIT assume il ruolo di “**stabilimento principale**”.

I server www.aeit.it, ammi.aeit.it, convegni.aeit.it, corsi.aeit.it, energiaelettrica.aeit.it sono contenuti in un armadio con chiusura a chiave di sicurezza. La rete a cui i due server sono connessi è totalmente ed esclusivamente di tipo cablato per minimizzare il rischio di connessioni non autorizzate.

AEIT non conserva alcun dato personale su sistemi cosiddetti “cloud” ed utilizza esclusivamente macchine che sono sotto il suo diretto controllo.

3. Danneggiamento dell'archivio

I server **www.aeit.it, ammi.aeit.it** e **corsi.aeit.it** che conservano l'archivio dei dati personali dei Soci e dei titolari di account di tipo “Guest” sono tre “macchine virtuali” ospitate da una macchina fisica (“macchina host”) che è dotata di coppie di dischi rigidi configurate in modalità RAID 1. Nella modalità RAID 1 i due dischi di una coppia contengono gli stessi dati creando così un sistema a ridondanza completa.

Grazie alla ridondanza completa della modalità RAID 1, qualora uno dei dischi della coppia dovesse andare fuori servizio per un guasto la macchina host e le macchine virtuali che ospita potrebbero continuare ad operare utilizzando il disco superstite nella coppia. In questo modo la probabilità di danneggiamento del database si riduce fortemente rispetto a situazioni senza ridondanza o con ridondanza parziale.

I server **convegni.aeit.it** e **energiaelettrica.aeit.it** sono ospitati da una macchina fisica dotata di una coppia di dischi rigidi configurata in modalità RAID 1. Nella modalità RAID 1 i due dischi di una coppia contengono gli stessi dati creando così un sistema a ridondanza completa. Se uno dei dischi della coppia dovesse andare fuori servizio per un guasto la macchina potrebbe continuare ad operare utilizzando il disco superstite nella coppia.

Al fine di ridurre ulteriormente le probabilità di danneggiamento dei database tutte le unità disco sono state scelte con particolare attenzione al parametro MTBF (“Mean Time Between Failures” o “tempo medio fra i guasti”) dichiarato dal costruttore. Tutte le unità disco utilizzate hanno MTBF maggiore di 1.000.000 ore.

Periodicamente i database dei server www.aeit.it, ammi.aeit.it e corsi.aeit.it che costituiscono l'archivio vengono sottoposti a back-up per ulteriore protezione contro il danneggiamento dell'archivio stesso.