



IRET - Policy di sicurezza informatica

Obiettivo e scopo

Questo documento descrive l'organizzazione e le procedure che devono essere seguite da tutto il personale che afferisce all'Istituto e che utilizza un computer o l'infrastruttura di rete dell'Istituto stesso. La mancata osservanza dei requisiti del presente documento, di eventuali procedure di protezione dei dati, della politica di utilizzo o di eventuali politiche e procedure di protezione delle informazioni trattate dall'Istituto potrebbe comportare la perdita dei privilegi di amministratore o la revoca stessa del computer assegnato e l'imposizione di eventuali sanzioni disciplinari.

Requisiti generali

Tutti i computer acquistati per o per conto di IRET sono di proprietà di IRET. Ogni membro dello staff a cui è stato assegnato un computer è responsabile della sicurezza di quel computer e delle informazioni in esso memorizzate, indipendentemente dal fatto che il computer sia utilizzato in ufficio, in un luogo di residenza o in qualsiasi altro ambiente esterno all'Istituto.

Al momento dell'assegnazione di un computer, tutti gli utenti dovranno leggere e firmare un documento in cui si dichiara di accettare di rispettare la politica e le procedure di sicurezza per l'utilizzo del computer indicate dall'Istituto.

La politica e le procedure saranno periodicamente aggiornate seguendo le eventuali variazioni di legge e/o modifiche nell'organizzazione d'Istituto che dovessero subentrare in futuro. A tutti gli utenti verranno fornite copie dei documenti relativi alla politica e alle procedure e saranno tenuti a rispettarne tutti i requisiti previsti.

Accesso limitato

Il computer assegnato è per uso esclusivo nell'esecuzione del proprio lavoro. Non è possibile condividere il computer con nessuno, inclusi altri colleghi IRET, familiari o amici.

Nessun uso personale o commerciale

Il computer assegnato può essere utilizzato solo per attività che rientrano nell'ambito di impiego presso IRET. Non è possibile utilizzare il computer per uso personale o commerciale.

Divieto di installazione del software

Gli utenti possono installare sul computer assegnato solo software autorizzato. Se fosse necessario installare altro software o modificare in altro modo la configurazione del computer, è necessaria l'autorizzazione del Direttore dopo consultazione con il gruppo informatico di IRET. Qualsiasi software non autorizzato sarà considerato come una violazione delle policy di sicurezza informatica e l'assegnatario del computer sarà individuato come responsabile per eventuali danni causati dall'applicativo al sistema informatico di IRET o al trattamento dati personali di cui l'Istituto è titolare o responsabile.



Le password

- Non condividere o divulgare la password.
- Non conservare nello stesso luogo la password e il computer e non memorizzare le password sul disco rigido del computer.
- Non consentire ai browser Web o alle applicazioni di archiviare password e informazioni di accesso.

Backup dei dati

I dati memorizzati sul disco rigido del computer (unità C) possono andare persi in quanto non automaticamente sottoposti a backup. I singoli utenti sono responsabili dei backup dei dati salvati sul pc. Se si lavora in remoto con VPN, accedere regolarmente alla rete e eseguire il backup dei dati su unità di rete. In caso di ulteriori domande sul backup dei dati, contattare il gruppo informatico. Se il computer dovesse venire portato in assistenza per riparazione effettuare un backup di sicurezza.

Dati riservati

- Posizionare computer, che visualizza informazioni riservate, in modo che lo schermo non possa essere visualizzato da altri.
- Se sul computer sono archiviate informazioni riservate, assicurarsi che non vengano trafugate e/o, se ritenuto opportuno, crittografate in un file o volume sicuro. Contattare il gruppo informatico se è necessario un software di crittografia.
- Tutti gli usi e le divulgazioni di informazioni riservate devono essere conformi alle regole deontologiche e alle leggi e normative applicabili.

Sicurezza in Istituto

- Non lasciare mai il computer incustodito per un periodo di tempo prolungato a meno che non sia riposto al sicuro in un armadio o in un ufficio chiuso a chiave.
- Disconnettersi sempre dal computer o premere Ctrl + Alt + Canc e selezionare "Blocca Workstation" quando ci si allontana anche per un breve periodo.

Sicurezza in viaggio

- Quando si è in viaggio, tenere il computer vicino e non lasciarlo incustodito.
- Disconnettersi sempre dal computer o premere Ctrl + Alt + Canc e selezionare "Blocca Workstation" quando ci si allontana anche per un breve periodo.
- Disconnettersi sempre dal computer e riporlo con tutte le periferiche in una custodia non visibile prima di trasportarlo tra le varie località.
- Non lasciare mai il computer incustodito in aree pubbliche.
- Evitare di lasciare il computer incustodito in un'automobile anche se il veicolo è bloccato, eventualmente riporlo nel bagagliaio.

Incidenti relativi al computer e/o di sicurezza

Se il computer assegnato viene smarrito, rubato o danneggiato contattare il gruppo informatico di Istituto il prima possibile. Inoltre è necessario segnalare eventuali incidenti legati alla sicurezza che coinvolgono il computer. Ciò consentirà all'Istituto di indagare e prendere provvedimenti per mitigare il rischio di eventuali perdite di dati riservati conservati sul computer.



Cura e manutenzione

Devono essere seguite le seguenti raccomandazioni su cura e manutenzione del computer:

- Aggiornamenti e patch antivirus: il computer deve essere aggiornato con gli ultimi aggiornamenti e patch antivirus.
- Fare attenzione a non urtare o far cadere il computer e non mettere oggetti sopra di esso tenendo tutti i liquidi lontano dal computer.
- Evitare di sottoporre il computer a sbalzi di temperatura estremi (temperature di esercizio da 10 a 35 °C e temperature di stoccaggio da -20 a 60 °C).
- Segnalare immediatamente eventuali problemi tecnici, relativi al computer, al gruppo informatico dell'Istituto.