POLITECNICO
MILANO 1863

DIPARTIMENTO DI ARCHITETTURA E STUDI URBANI

Linee guida per la gestione della sicurezza informatica

Sommario

Dipartimento di Architettura e Studi Urbani
Via Bonardi, 3
20133 Milano

Tel. 02 2399 5400-5401-5406
Fax 02 2399 5435
www.dastu.polimi.it
www.polimi.it

Partita Iva 04376620151
Codice Fiscale 80057930150

POLITECNICO
MILANO 1863

1. Postazioni informatiche e PC portatili/Tablet assegnati a personale docente

1.1 Sistema operativo

- Mantenere il sistema operativo costantemente aggiornato, verificando che l'installazione di patch e update siano andate a buon fine (MM_AGID_4.5.1)[1];
- evitare di modificare le impostazioni di sicurezza del sistema operativo abbassando i livelli di controllo (impostazioni di controllo account utente, antivirus, firewall, browser);
- si consiglia di utilizzare i punti di ripristino del sistema operativo o altro sistema analogo al fine di recuperarne le impostazioni in caso di malfunzionamenti.

1.2 Software

- Si raccomanda di installare solo software certificato e/o di provenienza affidabile (MM_AGID_2.1.1);
- MANTENERE i software aggiornati, soprattutto in caso di patch di sicurezza (MM_AGID_4.5.1)

1.3 Protezione

- Installare e attivare Antivirus e Firewall mantenendoli costantemente aggiornati (MM_AGID_8.1.1 e 8.1.2);
- effettuare regolari scansioni del sistema;
- disattivare esecuzioni automatiche/anteprime (ad esempio, autorun dischi rimovibili, apertura automatica di mail, abilitazione automatica di macro, anteprime allegati, anteprime immagini). (MM_AGID_8.7.1);

1.4 Gestione credenziali

- Evitare di utilizzare nomi utenti standard (es. administrator, root) in caso di utilizzo della macchina con pieni diritti di amministratore;
- proteggere il proprio computer con password robuste (ad esempio, contenenti caratteri minuscoli, maiuscoli, speciali e numeri), ricordando che la robustezza della password aumenta con il crescere del numero di caratteri utilizzati (esempio, una password di 14 caratteri è considerata robusta) (MM_AGID_5.7.1);
- conservare le password in un luogo sicuro e non accessibile a terzi (ad esempio in un unico file criptato o un password manager);
- si raccomanda di cambiare ogni 6 mesi le password non utilizzando password usate in precedenza (MM_AGID_5.7.3);
- usare password diverse per i login più importanti.

1.5 Accesso remoto

- Accedere alle risorse dati con protocolli di rete sicuri (ad esempio sono sicuri i protocolli usati dai NAS di dipartimento, che supportano AFS, NFS, SMB 3); evitare di accedere con protocolli non sicuri (es. FTP non criptato) perché le password possono essere intercettate;

[1] La sigla MM_AGID_X.X.X tra parentesi si riferisce alla corrispondente misura minima AgID per la sicurezza informatica.
L'elenco delle misure minime è consultabile sul sito ufficiale AgID al seguente link: https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

POLITECNICO
MILANO 1863

- accedere dall'esterno alle risorse del Dipartimento esclusivamente tramite VPN
- dipartimentale;
- per esigenze particolari sull'accesso remoto, ossia per l'utilizzo di protocolli diversi dalla VPN di Ateneo, rivolgersi al Referente ICT per lo studio di soluzioni sicure dal punto di vista informatico.

1.6 Dati

- Memorizzare i dati riservati localmente sul computer e/o su periferiche esterne usando partizioni criptate, che sono ormai disponibili in ogni sistema operativo ad esempio BitLocker per Windows o FileVault e le impostazioni di cifratura del disco per MacOs. Per dati personali, confidenziali o protetti da NDA si veda il paragrafo 3;
- effettuare un backup almeno settimanale su dispositivi diversi da quelli di archiviazione, (possibilmente non costantemente online) per evitare perdita di dati dovute a guasti hardware o infezioni tipo ransomware, virus e malware in grado di criptare tutti i file del PC con richiesta di riscatto. Si precisa che il sistema NAS dipartimentale è dotato di ulteriore backup offline.

1.7 E-mail

- Evitare l'apertura di allegati o link di mail la cui autenticità sia dubbia;
- ricordare che normalmente le mail provenienti da fonti ufficiali non richiedono di inserire i propri dati riservati o dati di accesso al servizio. Nel caso accadesse è comunque raccomandabile non cliccare il link ma digitare manualmente su un browser l'indirizzo a noi noto del sito istituzionale dal quale proviene la mail;
- phishing: in caso di dubbi sull'autenticità di un messaggio è consigliabile contattare il Referente ICT (evitando di inoltrare la mail).
  Alcuni esempi (non esaustivi) di messaggi anomali che potrebbero essere tentativi di phishing sono:
  - Mittenti non noti o domini sconosciuti o non ufficiali (esempio dominio ufficiale: @polimi.it, esempio di dominio non ufficiale: @polimi.esempio.it);
  - messaggio riportante palesi errori di grammatica o ortografica (riconducibili a tentativi di traduzione automatica);
  - link che riconducono a server non ufficiali (testo visualizzato del link non corrispondente all'indirizzo internet effettivo di destinazione).

In caso compromissione del sistema

Disconnettersi dalla rete, disconnettere eventuali risorse esterne (es NAS o archivi usb) ed eseguire immediatamente la scansione completa del sistema con antivirus. In caso di dubbi sulla efficace risoluzione del problema contattare il Referente ICT del Dipartimento.

POLITECNICO
MILANO 1863

2. Buone prassi per i PC condivisi (es: postazioni di laboratorio)

In aggiunta alle precedenti raccomandazioni si riportano le seguenti buone prassi per una corretta gestione dei PC di laboratorio:

- installare esclusivamente il software necessario per svolgere l'attività di ricerca;
- evitare di conservare dati di archivio (es. dati relativi a esperimenti obsoleti) direttamente sull'hard- disk della macchina e di spostarli in un archivio esterno (NAS, disco esterno);
- identificare un referente/responsabile del PC (dottorando/post-doc/ricercatore del gruppo);
- evitare di salvare e mantenere sui PC di laboratorio file contenenti dati personali o di terzi;
- evitare dove possibile l'utilizzo di programmi di email reading, social networking;
- per postazioni usate da più utenti comprendenti tesisti e ospiti valutare la possibilità di creare account utente con privilegi limitati;
- per i PC direttamente collegati ad apparecchiature scientifiche (controller, acquisizione dati), nel caso fosse necessario per motivi di compatibilità utilizzare sistemi operativi o altro software scientifico obsoleti, si raccomanda di mantenere tale PC disconnesso dalla rete.

Per il rispetto di tutti questi requisiti è possibile progettare, solo per i docenti che ne facessero esplicita richiesta, soluzioni specifiche (paragonabili a quelle adottate per i NAS di Dipartimento), con il supporto del Referente ICT.

3. Gestione delle informazioni riservate/protette da NDA e dei dati personali

Tenuto conto della responsabilità giuridica che il Dipartimento si assume nel momento in cui in Consiglio di Dipartimento viene approvato un NDA o un progetto che prevede trattamenti di dati riservati o personali sensibili, le prescrizioni riportate al punto 1 diventano prescrizioni inderogabili. È inoltre necessario ricorrere ad ulteriori misure di sicurezza finalizzate a minimizzare i rischi, come di seguito indicato.

3.1 Prescrizioni generali per dati personali e/o riservati

3.1.1 Conservazione dei dati e loro comunicazione o trasferimento

- Utilizzo di uno strumento sicuro di archiviazione:
  - NAS Dipartimentali;
  - Storage di ASICT;
  - NAS locali in grado di garantire medesimi livelli di sicurezza informatica (da progettare con Referente ICT).
- Divieto di conservazione dati su PC personali, portatili, chiavette e altri supporti informatici privi di adeguati strumenti di protezione.
- Utilizzo di FileSender per comunicare o trasferire dati ad utenti interni o esterni al Politecnico, impostando in presenza di dati personali o riservati,

la crittografia mediante password da comunicare tramite sistema alternativo rispetto alla posta elettronica (es SMS);
- Condivisione dei dati mediante OneDrive con accesso ai soli utenti autorizzati;

In alternativa: per esigenze di trasporto fisico dei dati (esempio non inviabili via mail per motivi di riservatezza o privacy) e/o per l'utilizzo dei dati al di fuori della sede Politecnico è prescritto l'uso di:

- Chiavetta criptata o altro supporto equivalente;
- PC con Hard Disk criptato.

3.1.2 Gestione Password

- Non lasciare il dispositivo informatico sbloccato in caso di assenza anche momentanea (per bloccare la postazione utilizzare le combinazioni ⊞win+L su Windows o Command+Control+Q su MacOS)
- EVITARE di memorizzare sul dispositivo e sui browser password di accesso al sistema e ai dati riservati e/o sensibili. È consigliato inserire manualmente le password ad ogni accesso, anche avvalendosi di un servizio di password manager;
- utilizzo esclusivo di password robuste (sono ritenute robuste le password che soddisfano i seguenti requisiti: minimo 14 caratteri, contenenti lettere maiuscole e minuscole, numeri e caratteri speciali);
- ADOTTARE sistemi di password aging e password history.

3.1.3 Accesso remoto

- Per impostare un sistema di accesso remoto a dati personali o riservati contattare il Referente ICT;
- accedere alla risorsa dati con protocolli di rete sicuri;
- accedere dall'esternoalle risorse del dipartimento esclusivamente tramite VPN Dipartimentale.

3.1.4 Sicurezza

- Backup settimanale con crittografia;
- garantire un sistema di archiviazione che permetta l'accesso ai dati esclusivamente alle
- persone formalmente autorizzate;
- si ribadisce che in caso di conservazione dei dati su proprio pc fisso/portatile o su supporto esterno essi devono essere criptati.

3.2 Prescrizioni specifiche per attività con trattamento di dati personali particolari

- Interagire con il Responsabile Gestionale, il Referente ICT e il Referente privacy di Dipartimento per l'analisi delle soluzioni tecnologiche, procedurali e contrattuali da adottare, al fine di assicurare la piena applicazione del GDPR;
- contattare il DPO (Data Protection Officer) di Ateneo nel caso di trattamenti che presentino un rischio elevato per i diritti e le libertà delle persone fisiche, valutando la necessità di DPIA (Data Protection Impact Assessment);

- prevedere opportune misure in caso di data breach (violazione degli archivi di dati);
- attenersi, nel corso dei trattamenti, a quanto stabilito contrattualmente e alle prescrizioni del GDPR.

3.3 Prescrizioni specifiche per attività con trattamento di dati riservati

- interagire con il Responsabile Gestionale e il Referente ICT di Dipartimento per l'analisi delle soluzioni tecnologiche, procedurali e contrattuali da adottare, al fine di garantire la piena applicazione delle linee guida di Ateneo sulla Riservatezza;
- Identificare a livello contrattuale (NDA o contratto di ricerca) il responsabile del trattamento dei dati;
- provvedere ad identificare il personale ricercatore autorizzato al trattamento dei dati riservati, facendo sottoscrivere un impegno al rispetto delle condizioni di riservatezza;
- adottare tutte le misure previste dai contratti assicurativi ai fini della copertura dei rischi associati agli NDA.

3.4 Riferimenti normativi di Ateneo

- REGOLAMENTO TRATTAMENTO DEI DATI PERSONALI E DELLA SICUREZZA ICT
- MODELLO ORGANIZZATIVO PRIVACY DEL POLITECNICO DI MILANO
- ISTRUZIONI OPERATIVE PER IL TRATTAMENTO DATI PERSONALI

Aggiornamento, 20.02.2023