UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA INFORMATICA

**LISTA DI REVISIONE**

| REVISIONE | DATA | DESCRIZIONE |
|---|---|---|
| Rev. 1 | Giugno 2019 | Prima edizione documento |
| Rev. 2 | Giugno 2024 | Seconda edizione documento |
| Rev. 3 | Settembre 2026 | Terza edizione documento |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| REDAZIONE | VERIFICA | EMISSIONE |
|---|---|---|
| Gruppo Sicurezza ICT della Direzione Sistemi Informativi (Ufficio RTD) e Assicurazione Qualità | Dario Montardi, Prof. Mirco Marchetti | Paola Michelini |

UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

# SOMMARIO

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# INFORMAZIONI GENERALI SULLA SICUREZZA INFORMATICA IN ATENEO

Per garantire la sicurezza della rete di Ateneo e dei sistemi informatici tutti gli **Utenti** (docenti, ricercatori, personale Tec-Amm, collaboratori, studenti, dottorandi) che utilizzano una postazione di lavoro collegata alla rete Unimore devono adottare le Misure Minime di Sicurezza (MMS) richieste dalla circolare AgID (Agenzia per l'Italia Digitale) del 18 aprile 2017 n. 2/2017 e implementate dalla propria struttura di afferenza, disponibile al link https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Tra l'altro, le MMS obbligano alla riservatezza delle password, all'utilizzo di un software antivirus/antimalware aggiornato, all'installazione di solo software autorizzato e all'aggiornamento costante del sistema operativo e degli applicativi in uso.

L'adeguamento è reso obbligatorio anche dalle Misure di Sicurezza previste dalla Direttiva (UE) 2022/2555 (NIS 2) a cui l'Ateneo è soggetto in quanto a febbraio 2025 è stato individuato dall'Agenzia di Cybersicurezza Nazionale (ACN) come ente importante per l'attività di ricerca svolta.

Gli Utenti sono invitati a rivolgersi

- ai **referenti informatici della propria struttura** (elenco alla pagina https://www.diag.unimore.it/referenti-informatici-di-struttura/) per informazioni tecniche
- ai **referenti di sicurezza della propria struttura** per verificare periodicamente tutte le raccomandazioni di sicurezza indicate dalla struttura di afferenza e per segnalare un abuso/incidente informatico (elenco alla pagina https://www.diag.unimore.it/referenti-di-sicurezza-delle-strutture/)

In particolare, **TUTTI gli Utenti** sono invitati a prendere visione

- delle politiche di sicurezza attivate in Ateneo e pubblicate su www.sicurezzaict.unimore.it alla voce "Normativa di Ateneo"
- della "Acceptable Use Policy" del Garr, la Rete Italiana dell'Università e della Ricerca, che indicano le attività ammesse e non ammesse sulla rete e a leggere e seguire quanto indicato di seguito nelle "RACCOMANDAZIONI DI SICUREZZA PER TUTTI GLI UTENTI".

Gli Utenti che possono amministrare dispositivi informatici perché a conoscenza di credenziali con diritti di super-utente/administrator sono considerati *amministratori di sistema* di tali dispositivi (postazioni di lavoro e ambienti server) e devono seguire le ulteriori indicazioni "RACCOMANDAZIONI DI SICUREZZA PER AMMINISTRATORI DI SISTEMA".

Le MMS richiedono l'utilizzo di configurazioni sicure standard per la protezione dei sistemi operativi (ABSC ID 3.1.1 3.2.1). Pertanto, per l'installazione e configurazione di un ambiente server seguire le indicazioni "RACCOMANDAZIONI DI SICUREZZA PER LE INSTALLAZIONI DI SERVER".

Analogamente, per le stampanti e le multifunzioni collegate in rete, seguire le indicazioni "RACCOMANDAZIONI DI SICUREZZA PER STAMPANTI".

Per i casi d'uso non previsti dalle MMS di Ateneo e dal presente documento, gli Utenti possono fare riferimento al documento *"Linee guida per la configurazione per adeguare la sicurezza del software di base"*, pubblicate sul sito di Agid, nel quale sono riportate le best-practice per la corretta gestione dei sistemi informatici nella Pubblica Amministrazione.

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA PER TUTTI GLI UTENTI

Le raccomandazioni di seguito valgono per tutti gli utenti che utilizzano dispositivi collegati alla rete Unimore.

- I dispositivi personali utilizzati per accedere alla rete o ai servizi di Ateneo devono utilizzare sistemi operativi supportati, essere aggiornati e protetti mediante PIN/password o autenticazione biometrica e, ove applicabile, cifratura del dispositivo
- Non utilizzare sistemi operativi, applicazioni, firmware o dispositivi che non ricevono più aggiornamenti di sicurezza dal produttore, salvo eccezioni formalmente autorizzate e accompagnate da adeguate misure compensative
- Utilizzare password lunghe, robuste e uniche per ciascun servizio e non riutilizzare password già utilizzate per altri servizi. Cambiare immediatamente la password quando vi sia il sospetto che sia stata compromessa, se ne viene richiesta la sostituzione per motivi di sicurezza, se è stata per qualche motivo comunicata a terzi o se si sospetta che abbia perso il requisito di segretezza
- Conservare tutte le proprie password in modalità sicura e protetta, per esempio utilizzando un password manager che salvi le credenziali con crittografia forte, non scriverle su fogli o post-it, non comunicarle a voce o via email ad alcuno
- Impostare sempre uno screen-saver con richiesta di password o altro meccanismo di sicurezza (es. utilizzare l'opzione "Blocca" in Windows che rimanda alla schermata di login senza disconnettere) per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea
- Quando possibile e se non indicato diversamente dagli amministratori di sistema (es. Thin client), spegnere la postazione di lavoro al termine dell'attività lavorativa giornaliera
- Assicurarsi che sia presente un antivirus/antimalware aggiornato su tutte le proprie postazioni di lavoro per evitare la diffusione di virus in rete
- Qualora non sia stato già impostato dall'amministratore di sistema, controllare che l'antivirus effettui la scansione dei file e dei supporti provenienti dall'esterno (per esempio, pendrive USB o altro dispositivo di storage esterno)
- Qualora non sia stato già impostato dall'amministratore di sistema, assicurarsi che il sistema sia continuamente aggiornato, installare le ultime patch di sicurezza del sistema operativo e del software installato
- Accedere alla posta elettronica prevalentemente via web in modo che si applichino le politiche di sicurezza impostate centralmente, evitando la configurazione dell'account

in client/app di posta elettronica la cui configurazione è totalmente a carico dell'utente finale (es. per ragioni di sicurezza è necessario configurarlo in modo che non apra automaticamente gli allegati)

- Non condividere mai le credenziali di un account di posta ma attivare l'accesso in delega ai collaboratori
- Prestare attenzione a messaggi di posta elettronica sospetti, di cui non si conosce il mittente e/o che contengono link sospetti o allegati non richiesti o che ingenerano un falso senso di urgenza: non aprire gli allegati, non seguire i link (vd. http://posta.unimore.it/attenzione-al-phishing/)
- Non approvare richieste di autenticazione MFA non originate personalmente. Diffidare anche da messaggi che chiedono di comunicare codici OTP, confermare notifiche di autenticazione o feedback, scansionare QR code per accedere a servizi e quelli che ingenerano un falso sentimento di urgenza magari ricorrendo alla verifica del messaggio senza reply, utilizzando canali alternativi e ritenuti affidabili (telefonando, per esempio, al mittente)
- Qualora non sia stato già impostato dall'amministratore di sistema, disattivare l'anteprima automatica dei contenuti dei file
- Qualora non sia stato già impostato dall'amministratore di sistema, disattivare l'esecuzione automatica di contenuti dinamici (es. macro) presenti nei file
- Utilizzare sistemi di cifratura per laptop, tablet, smartphone e supporti rimovibili (es. chiavette USB) che contengono informazioni rilevanti o dati personali, per salvaguardarli in caso di furto o smarrimento
- Utilizzare per l'archiviazione e la condivisione di dati di Ateneo esclusivamente su servizi cloud autorizzati. Prima di condividere file o cartelle verificare destinatari, permessi e durata della condivisione. Evitare collegamenti pubblici o accessibili a "Chiunque disponga del link", salvo effettiva necessità
- Non inserire in servizi di intelligenza artificiale generativa non autorizzati credenziali, dati personali, informazioni riservate, documenti interni o altre informazioni dell'Ateneo non destinate alla diffusione pubblica. Fare riferimento alle Linee guida di Ateneo per l'utilizzo di strumenti di intelligenza artificiale
- Segnalare ogni sospetto furto di credenziali, rilevamento virus, tentativo di intrusione o altro abuso ai referenti di sicurezza di struttura, il cui elenco è reperibile all'indirizzo https://www.diag.unimore.it/referenti-di-sicurezza-delle-strutture/
- Fare sempre riferimento ai referenti informatici di struttura per l'installazione e la configurazione di nuovi dispositivi

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA PER AMMINISTRATORI DI SISTEMA

Le raccomandazioni di seguito sono rivolte a chi ha accesso con diritti amministrativi / super-utente ad uno o più dispositivi (computer, portatili, server, stampante di rete, etc) collegati alla rete Unimore.

- Attenersi a quanto indicato nelle "RACCOMANDAZIONI PER TUTTI GLI UTENTI"
- Preferire sempre l'utilizzo di credenziali personali che non abbiano privilegi di amministratore per l'utilizzo ordinario del proprio computer
- In caso sia necessario utilizzare privilegi di tipo amministrativo di frequente per effettuare operazioni di installazione/aggiornamento/configurazione del sistema, è possibile includere il proprio account nei gruppi di amministratori di dominio o locali in caso di sistemi Windows, o includere il proprio account nel gruppo dei *sudoers* per i sistemi Linux/Unix e MacOS ma è raccomandato l'utilizzo di un account nominativo dedicato esclusivamente alle attività amministrative
- Se sono configurate credenziali di default nel dispositivo e negli applicativi, provvedere a modificare subito la password
- Se è necessario autorizzare più profili amministratore, mantenere l'elenco delle utenze amministrative. Ogni *credenziale* deve essere nominativa e riconducibile ad una sola persona
- Assegnare a utenti, applicazioni e servizi esclusivamente i privilegi strettamente necessari allo svolgimento delle attività previste e per il tempo necessario
- Se la postazione è utilizzata da più utenti, ove possibile, non creare utenti locali ma abilitare l'accesso tramite i sistemi di Single Sign On di Unimore (per es. LDAP, Active Directory, Shibboleth, ecc.)
- Quando possibile, consentire l'accesso solo a utenti identificati nel sistema di identity management di Ateneo ed eliminare i profili utente non necessari o dismessi
- Utilizzare password complesse per l'utenza amministrativa, di almeno 14 caratteri e cambiare la password frequentemente (es. ogni 6 mesi) se l'account non ha un secondo fattore di autenticazione. Al posto della password è raccomandato utilizzare un meccanismo di autenticazione più forte (chiavi ssh, certificati digitali, etc)
- Adottare misure di custodia e protezione adeguate per garantire la disponibilità e la riservatezza della password dell'utenza amministrativa in caso di necessità
- Non utilizzare la stessa password per utenze o servizi diversi
- Non comunicare le proprie password ad alcuno

- Evitare di salvare le password sul sistema operativo o su applicativi in uso
- Aggiornare costantemente sia il sistema operativo sia le applicazioni installate alle ultime versioni senza vulnerabilità note e alle ultime patch di sicurezza disponibili
- Verificare periodicamente la presenza di vulnerabilità note nei sistemi e negli applicativi installati e applicare con priorità gli aggiornamenti relativi a vulnerabilità critiche o attivamente sfruttate.
- Installare un antivirus/antimalware e tenerlo costantemente aggiornato
- Installare un firewall locale
- Installare solo software autorizzato dalla propria struttura e, nel caso di particolari esigenze, comunicare l'eccezione ai propri referenti informatici che inseriranno il software nella lista degli autorizzati e valuteranno se sono necessarie particolari misure di sicurezza
- Disabilitare il boot da rete, USB, dispositivi rimovibili, impostando una password per il BIOS e per la modifica del dispositivo di boot
- Abilitare solo le condivisioni in rete necessarie all'attività lavorativa e protette mediante l'utilizzo di credenziali di accesso
- Per l'eventuale amministrazione da remoto utilizzare solo canali di comunicazione sicuri
- Trasferire file solo in modo cifrato (SCP, SFTP, FTPS, Rsync Over SSH)
- Ove necessario, privilegiare l'utilizzo di certificati SSL emessi da CA attendibili, non utilizzare certificati SSL self-signed
- Effettuare una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino del sistema rispettando le valutazioni di RTO e RPO e, in sistemi in cui questa valutazione ancora manca, almeno settimanalmente e su sistema esterno
- Per i sistemi e i dati critici adottare una strategia di backup che preveda copie separate e almeno una copia offline, immutabile o comunque non direttamente accessibile dal sistema protetto. Verificare almeno annualmente l'effettiva possibilità di ripristinare dati e sistemi dai backup.
- Nel caso in cui la postazione di lavoro contenga dati con particolari requisiti di riservatezza, sensibili o strategici, impostare la cifratura del disco se permessa o applicare la protezione crittografica
- In caso di riuso, riassegnazione o dismissione di una postazione di lavoro, disinstallare il software con licenza installato e cancellare le informazioni contenute nel disco se non cifrate con password

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

## Avvertenze ulteriori in caso di amministrazione di NAS (Network Attached Storage)

Un NAS (Network Attached Storage) offre un'archiviazione centralizzata in rete in cui memorizzare i dati.

- **Servizi esposti**: Le normali NAS commerciali, appena installate, solitamente, espongono una ricca dotazione di servizi pubblicamente accessibili, è indispensabile spegnere e lasciare disattivato tutto ciò che non è indispensabile per le esigenze specifiche per cui è stato acquisito l'oggetto, quindi se, per esempio, si vuole fare condivisione di file con macchine windows sarà necessario il servizio SMB (Samba) e andranno quindi spenti tutti gli altri, come tftp, code di stampa, servizi multimediali, etc…
- **Firewalling**: tutti questi oggetti offrono un qualche tipo di firewall locale, le marche, modelli e versioni degli stessi sono troppi per poter dare delle linee guida puntuali, ma in linea di massima l'accesso tramite firewall va ristretto al solo elenco di indirizzi IP che effettivamente dovranno accedere ai servizi offerti, solo nel caso non sia effettivamente possibile realizzare un elenco puntuale è accettabile restringere gli accessi alla sola rete della struttura
- **Utenze**: la NAS deve poter offrire i suoi servizi solo ed esclusivamente all'utenza universitaria ed a nessun altro, per questo è indispensabile che ciascun utilizzatore sia identificato nel Sistema Identity di Ateneo. Questo passaggio è indispensabile.
- **Aggiornamenti**: i NAS vengono venduti con un periodo di aggiornamenti garantiti, questi devono essere fatti puntualmente, con controlli al massimo mensili ed applicazione degli aggiornamenti in maniera puntuale: questo implica l'interruzione del servizio per la durata degli aggiornamenti, ma garantisce che la macchina offra un profilo minimo accettabile di sicurezza. I controlli sulla disponibilità di nuove versioni sia del Sistema Operativo che degli applicativi installati (non solo gli utilizzati, ma anche quelli spenti, ma comunque installati) devono essere controllati al massimo una volta al mese, meglio se più frequentemente. Quando il periodo di aggiornamenti garantiti finisce, l'oggetto, deve essere sostituito ed il vecchio scollegato dalla rete pubblica di Ateneo.

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA PER LE INSTALLAZIONI DI SERVER

Per l'installazione e la configurazione del sistema operativo gli utenti che gestiscono proprie postazioni di lavoro o ambienti server devono seguire queste raccomandazioni:

- evitare l'uso di sistemi preinstallati di cui non si conosce in dettaglio la configurazione, se si usano immagini virtuali o preconfigurazioni modificare le credenziali di amministratore prima di collegare il sistema alla rete
- se possibile, impostare una password per accedere al BIOS e disabilitare nel BIOS il boot da CD/DVD o da USB
- installare solo versioni supportate e stabili evitando di installare versioni obsolete o versioni in fase di sviluppo
- installare il sistema operativo in maniera minimale
- rivolgersi ai referenti informatici della propria struttura per indicazioni sul corretto collegamento alla rete
- rimuovere i pacchetti software non utilizzati e disattivare i servizi non necessari
- assegnare una password robusta per le credenziali amministrative, cambiarla frequentemente se l'account non ha un secondo fattore di autenticazione e non riutilizzarla a breve distanza di tempo
- creare utenti locali con username nominali e non generiche, ogni utenza deve essere riconducibile ad una persona
- se la postazione è utilizzata da più utenti, ove possibile, non creare utenti locali ma abilitare l'accesso tramite i sistemi di Single Sign On di Unimore (per es. LDAP, Active Directory, Shibboleth, ecc.)
- configurare opportunamente il firewall per impedire, limitare e monitorare l'accesso a specifiche porte o servizi
- abilitare solo le condivisioni in rete necessarie all'attività lavorativa e protette mediante l'utilizzo di credenziali di accesso
- trasferire file solo in modo cifrato (SFTP/SCP/rsync su SSH o HTTPS/TLS, secondo il caso d'uso)
- evitare l'accesso in remoto via RDP, VNC o simili consentendolo solo in casi eccezionali alle utenze che ne hanno l'effettiva necessità
- Ove necessario, privilegiare l'utilizzo di certificati SSL emessi da CA attendibili, non utilizzare certificati SSL self-signed
- disabilitare protocolli e servizi non utilizzati (es. il servizio IPv6 se non esplicitamente richiesto)

- installare un antivirus/antimalware e prevedere scansioni periodiche
- attivare un sistema di alert in caso di anomalie del sistema
- al termine della configurazione eseguire un backup completo del sistema per ripristinarlo in caso di compromissioni e mantenerlo offline
- aggiornare costantemente il sistema operativo con le patch di sicurezza che si rendono disponibili
- limitare i privilegi di amministratore ai soli utenti che hanno le competenze e la necessità di modificare la configurazione dei sistemi
- mantenere l'inventario delle utenze amministrative
- limitare al solo proprietario l'accesso ai file che contengono dati con particolari requisiti di riservatezza o informazioni critiche come certificati personali, chiavi private etc
- in caso di compromissioni del sistema informare immediatamente i referenti di sicurezza di struttura, il cui elenco è reperibile all'indirizzo https://www.diaq.unimore.it/referenti-di-sicurezza-delle-strutture/
- verificare con i referenti informatici di struttura se è disponibile un log server locale o centralizzato su cui mantenere copia dei messaggi di log

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA PER LE INSTALLAZIONI DI SERVIZI WEB

- Nel caso di servizi che richiedono l'accesso riservato si raccomanda di
  - resettare la password di amministratore imponendo una password complessa di almeno 14 caratteri
  - impostare l'autenticazione SAML in modo che gli utenti autorizzati accedano via SSO con le credenziali Unimore
  - imporre un filtro sugli accessi in modo da limitare l'accesso solo agli utenti che ne hanno diritto
  - verificare periodicamente i log di autenticazione al servizio

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

# RACCOMANDAZIONI DI SICUREZZA PER STAMPANTI

- Modificare subito la password predefinita dall'interfaccia web di configurazione della stampante e le community string di SNMP (solo se usato)
- Comunicare l'indirizzo della stampante a supporto.rete@unimore.it, per l'inclusione nella lista degli indirizzi il cui accesso è filtrato dal firewall di bordo
- Configurare le Access Control List (ACL) della stampante per limitare l'accesso alle subnet o ai dispositivi autorizzati
- Utilizzare connessioni crittografate quando si accede all'interfaccia web di configurazione della stampante (HTTPS, SSH)
- Disabilitare servizi/protocolli non necessari (Telnet, HTTP, FTP, SNMP, …)
- Aggiornare il firmware delle stampanti alle versioni più recenti e alle ultime patch di sicurezza

Esempi di possibili protocolli da disabilitare:

- **IPv6**, da disabilitare, la rete di Ateneo si basa su IPv4
- **Bonjour**, da disabilitare, si tratta dell'implementazione di Apple del protocollo Zeroconf di IETF e si preferisce non utilizzarlo per evitare traffico non necessario sulle reti locali
- **Porta 9100** (o HP JetDirect, socket): la maggior parte dei servizi di stampa utilizza questo protocollo, in particolare i driver di HP, quindi potrebbe non essere possibile disabilitarlo
- **LPD**: LPD è utilizzato per la stampa da molti sistemi Unix e Linux. Tuttavia, molti possono ora utilizzare anche CUPS (Common UNIX Printing System), che consente la stampa tramite diversi protocolli. Se non si ha bisogno di LPD, occorre disabilitarlo.
- **IPP**: se il protocollo Internet Printing Protocol non è utilizzato nel proprio ambiente, disattivarlo
- **FTP**: alcune stampanti consentono di caricare documenti FTP per la stampa. Questa funzione non è utilizzata nella maggior parte degli ambienti e dovrebbe essere disabilitata
- **SMB**: la stampa SMB (Windows) spesso non è necessaria, poiché è gestita da altri protocolli, come JetDirect. Inoltre non è crittografata. Se possibile, disabilitare la stampa SMB
- **SMTP**: viene utilizzato per la scansione e l'invio di fax e può essere disabilitato se non richiesto. Se necessario occorre configurarlo in modo sicuro:

    - richiedendo all'indirizzo supporto.posta@unimore.it l'abilitazione dell'IP alla spedizione mediante il server di Google
    - configurando la spedizione mediante smarthost **smtp-relay.gmail.com**, senza autenticazione, utilizzando le porte 25, 587 o 465 con SSL abilitato
- **SNMP**; da disabilitare, a meno che non sia necessario il monitoraggio della stampante tramite questo protocollo: in tal caso, occorre utilizzare delle community string diverse da quelle di default (per SNMP v1/v2) o, meglio, utilizzare SNMP v3 con credenziali utente/password che rispecchino i criteri di sicurezza generali sulle credenziali utente