IMPOSTAZIONI DI DEFAULT DA POLICY CIGS PER I PC DELLO STAFF

- Password aging and history (9 mesi)
- Screen-saver con richiesta di password o altro meccanismo di sicurezza per proteggere l'accesso alla propria postazione di lavoro nel caso di assenza anche temporanea
- Antivirus Defender e firewall attivo.
- Disattivazione anteprima automatica dei contenuti dei file
- Boot da rete, USB, dispositivi rimovibili disabilitato

RACCOMANDAZIONI PER LO STAFF SENZA PRIVILEGI AMMINISTRATIVI SUL PROPRIO PC

- Conservare tutte le proprie password in modalità sicura e protetta, non comunicarle a voce o via e-mail ad alcuno
- Cambiare immediatamente una password che è stata per qualche motivo comunicata a terzi o che si sospetti abbia perso il requisito di segretezza
- Evitare di salvare la password di un servizio sul browser o su un'applicazione ma ridigitarla sempre ad ogni nuovo accesso
- Effettuare una scansione con l'antivirus di tutti i file e i supporti provenienti dall'esterno
- Nel caso di utilizzo di client di posta elettronica, configurarlo in modo che non apra automaticamente gli allegati
- 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, non aprire gli allegati, non seguire i link
- Segnalare ogni sospetto furto di credenziali, rilevamento virus, tentativo di intrusione o altro abuso ai referenti informatici di struttura
- Fare sempre riferimento ai referenti informatici di struttura per l'installazione e la configurazione di nuovi dispositivi
- Verificare periodicamente le raccomandazioni di sicurezza e gli alert pubblicati nei canali istituzionali di UNIMORE

RACCOMANDAZIONI DI SICUREZZA PER GLI AMMINISTRATORI DEL PROPRIO PC

Alcuni utenti, secondo le politiche adottate dalla struttura di afferenza, possono mantenere le credenziali di amministratore dei propri dispositivi (computer, portatili, server, stampante di rete, etc.).
Chi accede con profilo di amministratore è obbligato dalle MMS a seguire ulteriori raccomandazioni rispetto a quanto indicato nelle "RACCOMANDAZIONI PER TUTTI GLI UTENTI".

- Consentire l'accesso solo a utenti identificati nel sistema identity di Ateneo ed eliminare i profili utente non necessari o dismessi
- 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.
- Abilitare solo le condivisioni in rete necessarie all'attività lavorativa e impostare una password di protezione
- Per l'eventuale amministrazione da remoto utilizzare solo canali di comunicazione sicuri
- In caso di dismissione di una postazione di lavoro, disinstallare il software con licenza installato e cancellare le informazioni contenute nel disco se non cifrate con password

Il personale che intende essere l'amministratore del proprio PC, dovrà inviare al direttore la dichiarazione di assunzione di responsabilità compilata e firmata.

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Centro Interdipartimentale Grandi Strumenti - C.I.G.S.
www.cigs.unimore.it

Modena, lí …/… /…

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA ICT PER IL PERSONALE DEL CIGS

Il sottoscritto _____, in servizio presso il CIGS

CHIEDE

Di essere abilitato ad utilizzare con privilegi di amministratore la seguente postazione di lavoro

Nome di dominio del PC: _____ IP: _____

DICHIARA

- di aver ricevuto e letto la tabella MMS con le modalitá di applicazione predisposte dal CIGS
- di assumersi la responsabilità di eventuali problemi di sicurezza derivanti dalla non applicazione delle Misure Minime di Sicurezza

In fede, Visto,