INFORMATIVA SULLA SICUREZZA DEI DATI

a cura dell'area Tecnica

Tipologia dei dispositivi autorizzati	DISPOSITIVO PROPRIO DISPOSITIVO IUAV
Software autorizzati	- Non installare software proveniente da fonti non ufficiali - Utilizzare sistemi operativi per i quali attualmente è garantito il supporto da Iuav - Per accedere alle applicazioni del proprio ente può essere utilizzata la connessione Internet domestica di tipo "flat" (il cui costo non dipende dal traffico di rete) oppure lo smartphone come hotspot per consentire l'accesso ad Internet al pc di casa - Le applicazioni di Iuav sono raggiungibili da remoto, o in cloud, il dipendente può accedervi attraverso gli strumenti di lavoro. - Opzionalmente in taluni casi, ove indicato dal servizio infrastrutture ICT potrà essere necessario ricorrere all'attivazione di una VPN (Virtual Private Network, una rete privata virtuale che garantisce privacy, anonimato e sicurezza) verso l'ente,
Protezioni Hardware e software sui dispositivi mobili, laptop, workstation e server	- Bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro - Non cliccare su link o allegati contenuti in email sospette - Utilizzare l'accesso a connessioni Wi-Fi delle quali si conosce la provenienza e protette con password che ripettino le policy richiamate più avanti nel testo
Valutazione e correzione continua della vulnerabilità	- **NON** Collegare al pc dispositivi mobili (penna usb, hard disk esterno, etc.)
Uso appropriato dei privilegi di amministratore	- Assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alla password policy in uso presso Iuav - La password è strettamente personale e non deve essere comunicata e/o condivisa con nessun'altra persona - Qualora vi sia la ragionevole certezza che le credenziali assegnate siano state utilizzate da terzi, l'utente dovrà procedere al cambio immediato della password - Per la conservazione sicura delle credenziali di accesso è vietato memorizzarle su fogli di carta, documenti cartacei e file conservati all'interno della postazione di lavoro. - Nei limiti tecnici consentiti dai sistemi, la password: 1) deve essere di lunghezza non inferiore ad 8 caratteri oppure, nel caso in cui il sistema non lo dovesse prevedere, di lunghezza pari al massimo consentito; 2) deve essere obbligatoriamente cambiata al primo utilizzo e successivamente almeno ogni 6 (sei) mesi; 3) deve contenere, ove possibile, almeno 3 caratteri tra numeri, caratteri alfabetici in maiuscolo e minuscolo, e caratteri speciali (es. 1U@v); 4) deve essere sempre diversa da almeno le ultime 4 precedentemente utilizzate;5) non deve presentare una sequenza di caratteri identici o gruppi di caratteri ripetuti; 6) deve essere nota esclusivamente all'utilizzatore e non può essere assegnata e/o comunicata ad altri; 7) non deve contenere riferimenti agevolmente riconducibili all'utente o ad ambiti noti; 8) non deve essere basata su nomi di persone, date di nascita, animali, oggetti o parole ricavabili dal dizionario (anche straniere) o che si riferiscano ad informazioni personali; 9) non deve essere memorizzata in funzioni di log-in automatico, in un tasto funzionale o nel browser utilizzato per la navigazione internet. Ove tecnicamente possibile, i requisiti di cui ai punti da 1) a 5) devono essere imposti da meccanismi automatici del sistema.
Difese contro i malware	- Assicurarsi che i software di protezione del sistema operativo (firewall, antivirus, etc.) siano abilitati e costantemente aggiornati - Effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo utilizzato
Copie di sicurezza	

Protezione dei dati	-	Disconnettersi sempre dai servizi e dai portali Iuav dopo aver concluso la sessione lavorativa