



ISTITUTO COMPRENSIVO OPICINA
con lingua d'insegnamento slovena
VEČSTOPENJSKA ŠOLA OPČINE
s slovenskim učnim jezikom

P.le MonteRe/Nanoški trg, 2 - 34151 Opicina/Opčine - TS
Tel. 040211119
e-mail tsic818007@istruzione.it - tsic818007@pec.istruzione.it

TSIC818007
CF/FK 90135570324

Opicina/Opčine, 26/03/2020

Prot.n./Zapis št. 1458

LETTERA DI INCARICO

ai sensi del Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679)

AMMINISTRATORE DI SISTEMA

Il/La sottoscritto/a **Annamaria Zeriali** in qualità di Titolare del Trattamento dei Dati per conto dell' ISTITUTO COMPRENSIVO OPICINA - OPČINE conferisce a **Massimiliano Mucchiut** codice fiscale **MCCMSM72R21L424R** l'incarico di AMMINISTRATORE DI SISTEMA

A tal fine l'amministratore di sistema si impegna a:

Adottare sistemi di controllo che consentano la registrazione degli accessi (log) effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi;

Sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);

Monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;

Effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;

Sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;

attivare le credenziali di autenticazione ai soggetti incaricati del trattamento, su espressa indicazione del Titolare del trattamento dei dati personali, per tutti i trattamenti che vengano effettuati con l'utilizzo di strumenti informatici;

Fare in modo che sia prevista la disattivazione dei codici identificativi personali (user- id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;

verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati nei pc presenti nell'unità produttiva

individuare le politiche che dovranno essere adottate per garantire la massima protezione dei sistemi contro i virus informatici e verificarne l'efficacia ogni tre mesi;

proteggere gli elaboratori dal rischio di accesso da parte di personale interno privo di autorizzazione nonché da parte di soggetti esterni;

garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduca nel sistema informatico o telematico (art. 615-ter del Codice Penale);

predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte sua (nella sua qualità di amministratore di sistema); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;

Gestire le password di root o di amministratore di sistema;

Collaborare con il Responsabile del Trattamento dei Dati o in sua assenza con il Titolare del Trattamento dei Dati;

Informare il Responsabile del Trattamento dei Dati o in sua assenza con il Titolare del Trattamento dei Dati sulle non corrispondenze con le norme di sicurezza e su eventuali rischi o incidenti.

E a rispettare le seguenti prescrizioni per l'assolvimento del compito assegnato:

Il trattamento dei dati deve essere effettuato in modo lecito e corretto.

I dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta.

E' necessaria la verifica costante dei dati e il loro aggiornamento.

In ogni operazione di trattamento deve essere garantita la massima riservatezza ed in particolare:

divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del Data Controller;

l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;

la fase di raccolta dei dati dovrà essere preceduta dall'informativa e dal consenso rilasciato nella forma di legge all'interessato;

in caso di interruzione, anche temporanea del lavoro verificare che i dati siano inaccessibili ai non autorizzati;

le proprie credenziali di autenticazione devono essere riservate;

rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;

informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e/o personali;

raccogliere, registrare e conservare i dati sia cartacei che su supporto informatico avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge

Le operazioni di cui sopra possono essere operate da limitatamente ai trattamenti oggetto dell'incarico

Gli obblighi relativi alla riservatezza, alla comunicazione e alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Le prescriviamo di limitare il trattamento dei dati a quanto necessario ed indispensabile all'adempimento delle sue mansioni, osservando inderogabilmente le norme di legge e i regolamenti interni.

Dovrà operare osservando le direttive del Titolare del Trattamento dei Dati e del Responsabile del Trattamento dei Dati.

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto sono da lei dovuti in base al vigente contratto di lavoro.

La presente autorizzazione ha efficacia fino alla risoluzione del rapporto per qualsiasi causa oppure fino a modifica o revoca

Il Titolare del Trattamento dei Dati

L'Amministratore di sistema

Massimiliano Mucchiut, in qualità di Amministratore di sistema dichiara di essere a conoscenza di quanto stabilito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679) e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Privacy Impact Assessment in relazione ai compiti sopra indicati.