Politica di gestione dei dispositivi mobili e BYOD

EDUCatt
Ente per il Diritto allo Studio Universitario
dell'Università Cattolica

Largo Gemelli 1, Milano

Milano 2024

Redazione:	Approvazione:	Data approvazione:	Edizione:	Prot. nr:
Daniele Clarizia	AG	dicembre 2024	1.01	ND

Titolo documento: Politica di gestione dei dispositivi mobili e BYOD

EDUCatt - Ente per il Diritto allo studio Universitario dell'Università Cattolica

Codice Fiscale: 97489410155 - P. IVA: 06529660968

Iscrizione al Registro delle persone giuridiche private presso la Prefettura di Milano n. 14-12-1341 del 29 novembre 2016

Sede centrale: Milano | Largo A. Gemelli 1 | Sede operativa: via L. Necchi 9 | web: www.educatt.it | www.educatt.org

Presidenza | Direzione: tel. 02.7234.2415 | fax 02.80.53.215 | mail direzione.dsu@educatt.it

Comunicazione istituzionale e promozione: tel. 02.7234.3234 | 02.7234.3201 | mail comunicazione@educatt.it

Accoglienza studenti, informazioni e agevolazioni economiche: tel. 02.7234.2416 | fax 02.8718.1067 | mail info.dsu@educatt.it

Ristorazione: tel. 02.7234.2400 | mail ristorazione@educatt.org

Assistenza sanitaria e psicologica: Largo Gemelli 1 | tel. 02.7234.2217 | mail centro.sanitario.dsu@educatt.it

Soluzioni e strumenti - Libri: tel. 02.7234.3226 | mail librario.dsu@educatt.it (distrib.) | tel. 02.7234.2235 | mail editoriale.dsu@educatt.it (prod.)

Sede di Brescia: via Tosio 1

Accoglienza studenti, informazioni, ristorazione e agevolazioni economiche: tel. 02.7217.2604 | mail info.bs.dsu@educatt.it

Libri (distribuzione): Libreria Università Cattolica, via Trieste 17/D | tel. 030.2406.440 | fax 030.2406.441 | mail libreria-bs@unicatt.it

Sede di Piacenza: via dell'Anselma 7

Accoglienza studenti, informazioni, ristorazione, libri (distribuzione): tel. 0523.62.11.11 | fax 0523.579.416 | mail info.pc.dsu@educatt.it

Sede di Roma: Largo F. Vito 1

Accoglienza studenti, informazioni, ristorazione, libri (distribuzione): tel. 06.301.54.210 | fax 06.301.55.708 | mail info.rm.dsu@educatt.it

SportInCampus: tel. 06.305.01.20 | mail sportincampus@educatt.org

Sommario

1. Scopo e diffusione del documento

Scopo

Questo documento intende fornire informazioni sulle politiche, sugli standard e regole di comportamento dei lavoratori per l'utilizzo di dispositivi mobili aziendali e di proprietà personale (laptop, smartphone e/o tablet) per accedere ai servizi dell'Organizzazione.

La Fondazione EDUCatt ritiene l'uso dei dispositivi mobili, come smartphone, computer portatili e tablet, uno strumento prezioso per raggiungere l'obiettivo di una piena mobilità operativa, ossia la capacità di lavorare quando, dove e come meglio ritenuto per il raggiungimento degli obiettivi aziendali, e ne incoraggia l'uso.

Tuttavia, i dispositivi mobili, siano essi di proprietà personale o di EDUCatt, rappresentano anche un potenziale rischio per le informazioni e i sistemi IT. Un dispositivo smarrito può contenere una quantità significativa di informazioni riservate memorizzate localmente e può consentire accessi non autorizzati ad altri sistemi e reti.

Il presente documento stabilisce dunque i requisiti per tutti gli utenti che desiderano utilizzare dispositivi mobili, aziendali e di proprietà personale, per accedere alle reti, alle informazioni interne o ai servizi informatici della Fondazione con lo scopo di agevolare l'uso e ridurre i rischi per la sicurezza e l'integrità dei dati, proteggendo l'infrastruttura tecnologica della Fondazione EDUCatt e dell'Ateneo che la ospita.

Eccezioni limitate alle policies possono essere previste a causa dell'evoluzione tecnologica dei dispositivi, dei software di utilizzo e delle regole di accesso ai sistemi dell'Università Cattolica e di EDUCatt.

Diffusione

La presente procedura di definizione della politica di gestione dei dispositivi mobili e BYOD è destinata a tutti i lavoratori e i collaboratori della Fondazione EDUCatt cui viene assegnato un dispositivo mobile o che abbiano necessità di utilizzare un dispositivo personale per accedere ai dati o alle reti e utilizzare le risorse dell'Azienda. Il documento è disponibile al download diretto all'indirizzo www.educatt.it/documenti/EDUCatt_Policies-dispositivi-mobili-e-BYOD.pdf e ne è prevista la diffusione attraverso comunicazioni online e la consegna, ove necessario, in fase di stipula dei nuovi contratti/incarichi da parte della funzione Risorse Umane.

Riferimenti normativi e documenti di base

- Procedura EDUCatt per la gestione interna e la comunicazione all'esterno di documenti e informazioni [EDUCatt_DATI_DEF_v8x_2017UE]
- Protocollo EDUCatt PT6 - Gestione e utilizzo del Sistema Informativo
- UCSC - Disciplinare sull'utilizzo delle risorse informatiche
- UCSC Procedura - Gestione accesso ai sistemi informatici

2. Definizioni e politiche esistenti

Definizioni

Postazione/dispositivo mobile di proprietà dell'azienda: EDUCatt fornisce a utenti autorizzati che ne hanno bisogno **smartphone, computer portatili e tablet aziendali**, configurati con software di base e specifici per uso aziendale, lasciando loro il pieno controllo (livello administrator) e le conseguenti responsabilità di gestione e della corretta funzionalità delle postazioni. I dispositivi mobili di questo tipo restano di proprietà esclusiva di EDUCatt e possono essere richiamati dal reparto IT per aggiornamenti o sostituzioni.
I dispositivi mobili forniti dall'azienda possono essere utilizzati dai lavoratori solo durante il periodo del loro rapporto di lavoro con l'azienda e, per le finalità accettate, anche in mobilità ovvero al di fuori degli uffici EDUCatt.
BYOD: i **dispositivi mobili di proprietà personale** sono ammessi all'interno dell'azienda e possono connettersi ai sistemi informatici e alle piattaforme software, nel rispetto delle norme generali di connettività e sicurezza emanate da EDUCatt e dall'Università Cattolica senza limitazioni di tipologia.
L'utente deve garantire che i dispositivi personali rispondano a requisiti analoghi a quelli richiesti per i dispositivi aziendali.
L'uso dei dispositivi mobili personali può essere limitato in base alla tecnologia utilizzata. Per qualsiasi informazione è possibile contattare il reparto IT EDUCatt all'indirizzo email ict@educatt.org.

Politiche esistenti

Le policies elencate in questo documento non devono ritenersi sostitutive di alcuna altra politica esistente in EDUCatt.

3. Usi e ambiti di applicazione

Usi accettabili e/o consentiti

EDUCatt ritiene uso aziendale accettabile le attività che supportano direttamente o indirettamente l'attività dell'Organizzazione, tendenzialmente da effettuarsi in orario lavorativo. In orario di lavoro è consentito un uso personale accettabile limitatamente a una misura ragionevole e contenuta nel tempo.
I dispositivi aziendali e i BYOD non devono essere in ogni caso utilizzati per memorizzare o trasmettere materiale illecito, molestare altre persone, compiere azioni dannose per altri utenti o per l'Organizzazione, diffondere informazioni false o virus, trojan e analoghi.
Si ricorda che non è consentita la scrittura o la gestione di messaggi o e-mail durante la guida, e che durante la guida è consentito l'uso dei dispositivi mobili esclusivamente a mani libere.

Dove tecnicamente possibile, EDUCatt può far rispettare l'uso accettabile tramite varie tecnologie all'interno della rete e richiedere l'installazione di software specifici sui dispositivi degli utenti, inclusi: a. Filtro URL (blocco dell'accesso a particolari classi di siti web, inclusi pornografia, così come siti che includono atti criminali, gioco d'azzardo, hacking, discorsi d'odio, violenza o armi) b. Anti-Malware (blocco di virus e altri software dannosi) c. Blocco degli allegati (blocco di determinati tipi di traffico email, anche in assenza di una minaccia specifica, come l'invio di programmi eseguibili) d. Prevenzione delle intrusioni (blocco del traffico che sembra essere dannoso) e. Gestione del traffico (blocco o rallentamento del traffico che viola la politica, come la condivisione di file peer-to-peer)
Queste limitazioni potrebbero applicarsi ai dispositivi BYOD anche quando utilizzati per scopi non lavorativi.
Le tecnologie di controllo includono la registrazione degli accessi e, in alcuni casi, l'identificazione dell'utente. I log potrebbero essere esaminati dal reparto ITC di EDUCatt e/o dell'Università Cattolica ed essere resi disponibili ad autorità in caso di necessità.

Ambito di applicazione

I dispositivi mobili autorizzati, siano essi di proprietà di EDUCatt o dell'utente, possono essere utilizzati per accedere a:

- reti di EDUCatt o dell'Università Cattolica (wireless o cablate, o da remoto);
- sistemi informativi interni e i servizi basati su cloud;
- informazioni riservate o privilegiate di EDUCatt.

Queste policies si applicano a tutti i lavoratori in possesso di BYOD, che siano a tempo pieno, part-time o legati da formule contrattuali differenti, in tutte le sedi, indipendentemente dal metodo di connessione utilizzato (reti wireless aziendali, connessioni internet domestica o connessione cablata presso gli uffici, ecc.).

Le regole qui esposte non sono normalmente applicabili alle postazioni desktop standard condivise gestite dall'Università Cattolica o da EDUCatt, poiché la politica di sicurezza e accesso per quei sistemi è gestita dal settore IT dell'Ateneo e di EDUCatt e non è sotto il controllo diretto dell'utente (livello user).

Attenzione: come parte di questa policy, l'azienda potrebbe bloccare i dispositivi degli utenti BYOD in modo che non possano essere utilizzati e può cancellare dati o contenuti sui dispositivi degli utenti BYOD, in caso di accessi o utilizzi sospetti o non autorizzati ai sistemi. Queste azioni potrebbero verificarsi anche accidentalmente.

Dispositivi ammessi e/o supportati

È ammesso l'uso dei seguenti dispositivi:
iPhone, iPad, Android, Windows, Mac, Linux.
Normalmente e dove possibile i problemi di connettività dei dispositivi mobili aziendali sono supportati dal reparto ITC EDUCatt (ict@educatt.org); per configurazioni e connettività sulla telefonia è necessario rivolgersi al settore reti e smartphone (Roberto Mariani). Per problemi legati al sistema operativo o all'hardware personale è necessario contattare il produttore del dispositivo o il proprio operatore.
Gli utenti BYOD sono responsabili dell'identificazione del proprio fornitore di servizi vocali/dati. EDUCatt non gestisce servizi vocali o di dati per i dispositivi BYOD.

Prima di accedere alla rete aziendale è consigliabile contattare il reparto ITC EDUCatt per la configurazione delle applicazioni standard, come browser, software di produttività per ufficio e strumenti di sicurezza.
EDUCatt non è tenuto a fornire supporto per i dispositivi BYOD. Il supporto disponibile è comunque limitato alle applicazioni ammesse e alle configurazioni di sicurezza/rete utilizzate per connettersi alle risorse aziendali.

Costi per l'uso dei dispositivi personali

I costi di tutti i dispositivi BYOD, compresa la stipula del contratto di utenza, il servizio vocale/dati, gli aggiornamenti hardware e le garanzie di manutenzione o di sostituzione in caso di furto, sono a carico dei rispettivi proprietari.
I costi dei dispositivi aziendali e dei relativi contratti d'uso sono a carico dell'azienda per tutti gli usi leciti sia sul territorio nazionale che internazionale (roaming).

4. Responsabilità

EDUCatt e gli utenti condividono la responsabilità per la salvaguardia delle informazioni lavorative. Gli utenti devono dunque esercitare in ogni momento la dovuta cura riguardo alla sicurezza delle informazioni e alla sicurezza fisica dei dispositivi.

Protezione dei dati

La Politica di gestione del sistema informativo di EDUCatt è indicata nell'apposito Protocollo *PT6 - Gestione e utilizzo del Sistema informativo*, richiamato tra i riferimenti normativi e i documenti di base e si applica a tutti i dispositivi mobili e agli utenti BYOD.
Le informazioni aziendali restano sempre di proprietà di EDUCatt, che si riserva il diritto di modificare o revocare in qualsiasi momento l'accesso o cancellare le informazioni riservate dai dispositivi BYOD.

Sicurezza del dispositivo mobile

I dispositivi mobili aziendali e BYOD devono essere trattati in ogni momento come beni fisici di valore e gli utenti devono prendersi cura di proteggere questi dispositivi da danni o accessi inappropriati. Gli utenti devono seguire le seguenti indicazioni:

- La condivisione dei dispositivi, anche con membri della famiglia, non è consentita ovvero i dispositivi devono utilizzare una tecnologia appropriata per separare i dati, l'accesso e le applicazioni di EDUCatt dall'uso domestico.
- Gli utenti BYOD non devono caricare software o contenuti piratati o illegali sui dispositivi BYOD, anche quando sono in uso profili Lavoro/Home.
- Gli utenti BYOD non devono tentare di eludere la sicurezza del produttore attraverso il jailbreak o rooting dei propri dispositivi.
- Gli utenti devono garantire che l'accesso e le credenziali memorizzate sui dispositivi non siano compromessi e che i dati riservati di EDUCatt non siano esposti a personale non autorizzato.

Perdita del dispositivo mobile

In caso di furto o smarrimento di un dispositivo aziendale, l'utente è tenuto a presentare denuncia alle autorità competenti e fornire copia della denuncia all'azienda, che provvederà alla sostituzione del dispositivo e alla disattivazione/riattivazione delle utenze.

Il dispositivo mobile smarrito/perduto/rubato, se di proprietà dell'azienda, potrà:

- essere bloccato in modo che non possa essere consentito l'accesso, anche con credenziali corrette (blocco del codice IMEI);
- cancellato in maniera definitiva da remoto (ripristino alle impostazioni di fabbrica).

Attenzione: Si consiglia agli utenti di intraprendere le stesse azioni appena indicate anche in caso di smarrimento, furto o perdita di un dispositivo personale. Le azioni sul dispositivo, volte a garantire la sicurezza delle informazioni aziendali, potrebbero causare la perdita permanente di eventuali dati personali memorizzati.

5. Sicurezza delle informazioni e privacy

Sicurezza

Gli utenti dei dispositivi mobili sono tenuti a installare i software di gestione indicati dall'Azienda per l'accesso alle informazioni aziendali e sono tenuti al rispetto delle misure di sicurezza e delle restrizioni raccomandate da EDUCatt nel Protocollo *PT6 - Gestione e utilizzo del Sistema informativo*.
Per evitare accessi non autorizzati, i dispositivi devono essere protetti da password forti o sistemi di accesso biometrici, utilizzando le funzioni del dispositivo.
Per accedere alla rete aziendale è necessaria l'autenticazione prevista dall'Università Cattolica, con l'uso di un una password forte e l'attivazione dell'autenticazione a più fattori.
Tutti i dispositivi devono essere crittografati.
È consigliabile attivare il blocco automatico del dispositivo in caso di inattività.
I dispositivi rootati (Android) o jailbroken (iOS) e i computer portatili, gli smartphone e i tablet che non figurano nell'elenco dei dispositivi supportati dall'azienda non possono connettersi alla rete.
Non è possibile connettere alla rete dispositivi degli utenti destinati esclusivamente all'uso personale, a meno di autorizzazione esplicita del Reparto ITC di EDUCatt.
I dispositivi aziendali possono essere cancellati da remoto se vengono persi, smarriti o rubati o se il lavoratore termina il suo rapporto di lavoro con EDUCatt o se viene rilevata una violazione dei dati o dei criteri, un virus o una minaccia simile alla sicurezza dei dati e dell'infrastruttura tecnologica dell'azienda.
È necessario che gli utenti garantiscano l'aggiornamento costante dei dispositivi BYOD con le ultime versioni del sistema operativo e delle applicazioni e che verifichino l'applicazione degli aggiornamenti periodici sui dispositivi aziendali affidati.

Privacy

EDUCatt rispetta la privacy degli utenti dei dispositivi mobili e BYOD e richiederà autorizzazione all'accesso, anche remoto, al dispositivo soltanto in caso di necessità per la risoluzione di problemi segnalati dall'utente, l'implementazione o la verifica di controlli di sicurezza o per rispondere a richieste legittime di scoperta derivanti da procedimenti amministrativi, civili o penali.
EDUCatt consiglia caldamente di utilizzare i sistemi cloud autorizzati (onedrive, dropbox) per la registrazione dei dati aziendali e di non registrare localmente i dati sui dispositivi. È consigliabile in ogni caso che gli utenti provvedano a backup periodici dei dispositivi affidati o dei BYOD, anche nelle aree cloud aziendali con accesso personale. Qualora tali backup includessero dati personali e privati, ivi comprese fotografie, registri di messaggi di testo, email private da server non aziendali, informazioni di contatto/indirizzi e altri dati non lavorativi, potrebbero essere visibili agli amministratori di sistema o al personale ITC di EDUCatt.

I dispositivi mobili o BYOD potrebbero segnalare l'uso, comprese le URL visitate e i dati sulla posizione, ai server di EDUCatt. In quel caso i files di log potrebbero essere esaminati dal personale ITC per scopi di debugging o risoluzione dei problemi.

6. Cessazione del rapporto di lavoro

In caso di dimissioni o cessazione del rapporto di lavoro, il lavoratore è tenuto a restituire il dispositivo di proprietà di EDUCatt. I dati su tale dispositivo verranno completamente cancellati ripristinando il dispositivo alle impostazioni di fabbrica.
L'Organizzazione non è responsabile per la eventuale perdita di dati personali memorizzati nel dispositivo di proprietà di EDUCatt. Nel caso di un dispositivo mobile di proprietà personale, il Lavoratore dovrà eliminare tutte le applicazioni e i dati di EDUCatt da tale dispositivo.

7. Restrizioni e violazioni

Restrizioni

Si ricorda che per garantire il corretto uso delle risorse e dei dati è necessario evitare di:
a. trasferire dati o informazioni di proprietà di EDUCatt a servizi o applicazioni basati su cloud non approvati dall'Organizzazione;
b. esportare, trasferire o sincronizzare i dati su BYOD destinati esclusivamente all'uso personale, condivisi o accessibili a familiari o terzi;
c. installare sui dispositivi mobili aziendali o sui BYOD in aree accessibili o utilizzate per lavoro applicazioni illecite o non approvate dall'Organizzazione;
d. applicare o apportare modifiche non approvate all'hardware o al software dei dispositivi aziendali

Rischi e responsabilità

È responsabilità degli utenti prendere tutte le precauzioni ritenute necessarie o idonee, aggiuntive a quelle indicate nel presente documento, per evitare la perdita di dati relativi all'Azienda.
L'utente è tenuto a utilizzare sempre i dispositivi in modo eticamente corretto, assumendosi la piena responsabilità per i rischi che includono la perdita parziale o totale dei dati aziendali e personali a causa di un crash del sistema operativo, errori, bug, virus, malware e/o altri guasti del software o dell'hardware, o errori di programmazione che rendono il dispositivo inutilizzabile.
EDUCatt si riserva il diritto di scollegare i dispositivi o disattivare i servizi senza preavviso e di adottare le opportune misure, anche amministrative o disciplinari, in caso di mancata osservanza o di violazioni di questa Policy o di altre correlate.