UOC Servizio Informatico e della Transizione Digitale
Direttore Dr. Massimo Iacono

REGOLAMENTO SUGLI ACCOUNT AZIENDALI

Redazione	Ufficio Privacy -Dr. Domenico Arezzo-
Verifica	Gruppo di lavoro Infrastrutture e Sicurezza IT
Approvazione	Direttore UOC -Dr. Massimo Iacono-
Nome del documento	Regolamento sugli account aziendali
Data del documento	11/11/2024
Versione del documento	1.0
Allegati	Documento responsabile del trattamento (Microsoft)

Sommario

1. Contesto

1.1 Perimetro

L'Azienda Sanitaria Provinciale di Ragusa (di seguito "**ASP**"), per il tramite dell'Ufficio Privacy e del Servizio Informatico e della Transizione Digitale (di seguito "**SITD**"), ha definito e predisposto il presente Regolamento sugli account aziendali (di seguito "**Regolamento**") tramite cui sono definite le regole e i principi per la corretta gestione degli account (utenze) aziendali, sia di posta elettronica che di dominio, degli utenti che operano con le piattaforme informatiche dell'ASP (dipendenti e collaboratori).

Detto Regolamento viene pubblicato e aggiornato sul sito Aziendale insieme ad Allegati e istruzioni aggiuntive tra cui quelli volti a disciplinare i diritti, le modalità di accesso e il ciclo di vita delle autorizzazioni concesse a soggetti interni ed esterni all'ASP per l'accesso ai diversi sottosistemi applicativi e alle device (pc/tablet).

1.2 Responsabilità connesse

Direttore U.O.C. SITD	Massimo Iacono
Infrastruttura e Sicurezza	Gruppo di lavoro
Gestione degli Applicativi	Giancarlo Cappello
Gestione per il trattamento dati – Ufficio Privacy-	Domenico Arezzo
Software di comunicazione Office365 email/teams/Bi	Fornitore Microsoft

2. Definizioni

- **ASP**: Azienda Sanitaria Provinciale di Ragusa
- **Autorizzazioni**: livelli di accesso a cui si è abilitati in funzione del ruolo
- **Dominio**: Strumento per la gestione degli account per l'accesso alle risorse ICT aziendali (server, le postazioni di lavoro (PC), le diverse device collegate, gli applicativi, il cloud).
- **GDPR:** Regolamento Generale per la Protezione dei Dati Personali UE 2016/679
- **ICT:** Information Communication Telecomunication
- **RUP:** Responsabile Unico del Procedimento
- **Single Sign-on**: ambiente unico di autenticazione a cui sono collegati i permessi ai diversi applicativi

- **SITD:** Servizio Informatico e della Transizione Digitale
- **U.O.C:** Unità Operativa Complessa
- **U.O.S.D:** Unità Operativa Semplice Dipartimentale
- **U.O.S:** Unità Operativa Semplice
- **Utente interno:** il dipendente/collaboratore che ha un contratto di lavoro a tempo indeterminato/determinato ovvero un contratto di collaborazione, un'assegnazione in presidio, un contratto di consulenza, uno specifico incarico (anche se non remunerato) che lo vede impegnato all'interno dell'ASP. In ogni caso, gli incarichi predetti dovranno contemplare la necessità di accedere ai servizi informatici dell'ASP.
- **Utente esterno:** il dipendente/professionista convenzionato con l'ASP per attività che coinvolge le piattaforme informatiche dell'ASP. Esempi di utente esterno: MMG e Pediatri di Libera scelta, Farmacie, Convenzionati esterni, strutture su cui opera personale di intramoenia, CAAF, Comune, Associazioni.

3. Normativa e Linee Guida

- Legge del 20 maggio 1970, n. 300 (Statuto dei lavoratori)
- Linee guida del Garante per la protezione dei dati personali per posta elettronica e internet - 5 marzo 2007
- Provvedimento del Garante per la protezione dei dati personali n. 216 - 4 dicembre 2019
- Linee guida del Comitato europeo per la protezione dei dati personali (EDPB) 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR
- Provvedimento del Garante per la protezione dei dati personali n. 42 - 10 febbraio 2022
- Provvedimento del Garante per la protezione dei dati personali 22 febbraio 2024, n. 127, doc. web n. 9987885; Gazzetta Ufficiale n. 64 del 16 marzo 2024
- Provvedimento del Garante per la protezione dei dati personali n. 140 - 7 marzo 2024
- Provvedimento del Garante per la protezione dei dati personali "Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" - 6 giugno 2024
- Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, recante le misure minime di sicurezza ICT per le pubbliche amministrazioni
- Direttiva (UE) 2022/2555 -NIS2 sulle misure per un livello comune elevato di cybersecurity in tutta l'Unione Europea –
- Linee guida per il rafforzamento della resilienza dei soggetti di cui all'articolo 1, comma 1, della Legge 28 giugno 2024, n. 90

4. Attività

4.1 Inquadramento introduttivo

Gli account aziendali sono relativi al dominio, agli applicativi e alla posta elettronica e vengono assegnati all'utente al momento dell'instaurazione del rapporto di lavoro/collaborazione/convenzione.
L'utente con account viene abilitato alle procedure di competenza a seconda del ruolo, qualifica, UO di assegnazione e mansioni.

4.2 Ciclo di vita degli account aziendali e delle autorizzazioni all'accesso agli applicativi

a) Premessa

Gli account aziendali di dominio permettono all'utente l'accesso alla propria postazione di lavoro.
Le credenziali di accesso al dominio, posta elettronica e dell'applicativo, in modo equivalente all'apposizione di una firma debole, permettono la tracciabilità delle operazioni eseguite secondo il livello di dettaglio previsto in ogni singola piattaforma.

L'account aziendale di posta elettronica permette all'utente di gestire:

- la propria casella di posta elettronica aziendale;
- l'accesso e l'utilizzo dei servizi correlati alla piattaforma Microsoft Office365 in relazione alla licenza assegnata.

b) Creazione e attivazione dell'account aziendale di dominio e di posta elettronica

La creazione e l'attivazione dell'account aziendale di posta elettronica e di dominio dell'utente è a carico del SITD, a cura dell'Amministratore del sistema, al momento dell'instaurazione del rapporto di lavoro dipendente/collaborazione/convenzione. L'ASP individua e nomina gli Amministratori di Sistema in conformità al provvedimento del Garante per la protezione dei Dati Personali del 27 novembre 2008, pubblicato in G.U. n. 300 del 24.12.2008.

La pratica deve essere attivata, previa esecuzione degli adempimenti privacy (Vedi allegato "1 - Privacy"), dall'ufficio personale dell'ASP o dell'ufficio che attua il contratto di convenzione/incarico al momento della stipula dell'incarico stesso/contratto.

Il Responsabile dell'U.O.C./U.O.S.D./U.O.S. presso cui l'utente svolge la propria attività lavorativa, previa esecuzione degli adempimenti privacy (Vedi allegato "1 - Privacy") deve richiedere gli accessi, le integrazioni e le revoche degli account di ciascuna piattaforma di competenza.

Il paragrafo precedente è esteso al RUP del contratto di affidamento dell'attività per il personale non dipendente dell'ASP.

c) Reset della password

Per la gestione del reset della password vedere il manuale di istruzioni (allegato "2 – Reset") presente sul sito aziendale.

d) Cessazione dell'account aziendale di posta elettronica e di dominio e dell'autorizzazione all'accesso agli applicativi

L'account aziendale rimane attivo finché l'intestatario ha un contratto in essere con l'ASP.

La disattivazione, per gli account assegnati al personale con matricola avviene in automatico in corrispondenza al giorno successivo alla data di fine servizio ad eccezione di quegli applicativi indicati nell'allegato "3 - credenziali applicativi" in cui la disattivazione deve essere richiesta da un referente.

La disattivazione, per gli account assegnati per il personale senza matricola avviene su specifica richiesta del RUP o del referente del contratto a cui è collegata l'utenza.

L'account aziendale di posta elettronica ha carattere personale ma non "privato", in quanto trattasi di strumento di esclusiva proprietà aziendale messo a disposizione dell'utente al solo fine dello svolgimento delle proprie mansioni lavorative. Pertanto, in caso d'interruzione del rapporto di lavoro:

- l'indirizzo di posta elettronica dell'utente viene disabilitato in corrispondenza al giorno successivo alla data di fine rapporto.
- l'indirizzo di posta elettronica dell'utente viene bloccato e disabilitato come previsto dal par. 8.6 del "Regolamento aziendale per l'uso di strumenti informatici, internet e posta elettronica e per la tutela dei sistemi informativi";
- il contenuto (file e corpo del messaggio) dell'account di posta elettronica viene disabilitato, in conformità agli artt. 5, par.1 lett. a) ed e), 88 del GDPR e agli artt. 113 e 114 del D.lgs. 196/03

Qualora l'utente venga assegnato ad altre mansioni o riassegnato presso sedi dell'ASP diverse rispetto a quella originaria, l'accesso agli applicativi viene bloccato secondo quanto indicato nell'allegato "3 - credenziali applicativi".

La disabilitazione dell'accesso agli applicativi non pregiudica l'utente nell'utilizzo dell'account aziendale di dominio, nella sua funzionalità di base, e di posta elettronica.

4.3 Gestione dei contenuti, dei metadati e dei log

4.3.1 Criteri per la raccolta e conservazione dei medatadati e dei log di dominio

I log relativi agli accessi di autenticazione tramite SSO, nonché i log e i metadati presenti all'interno degli applicativi in uso presso l'ASP sono conservati secondo i criteri e nel rispetto dei temi previsti nell'allegato "3 - credenziali applicativi"

4.3.2 Criteri per la raccolta e conservazione dei dati negli account aziendali di posta elettronica

I dati oggetto di raccolta e conservazione nella gestione aziendale della posta elettronica fanno parte di tre categorie:

- **contenuto** (corpo del messaggio e file), come definito dal Garante per la protezione dei dati personali (nel seguito "**Garante**") nel Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati: "*le informazioni contenute nell'envelope, ancorché corrispondenti a metadati registrati automaticamente nei log dei servizi di posta, sono inscindibili dal messaggio di cui fanno parte integrante e che rimane sotto l'esclusivo controllo dell'utente (sia esso il mittente o il destinatario dei messaggi*)"; pertanto il contenuto (file e corpo del messaggio) dell'account di posta elettronica viene cancellato a 30 giorni dalla conclusione del rapporto di lavoro, in modo automatizzato. Difatti, come indicato dal Garante nel Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati: "*il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati - riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.), che proteggono il nucleo essenziale della dignità della persona e il pieno sviluppo della sua personalità nelle formazioni sociali. Ciò comporta che, anche nel contesto lavorativo pubblico e privato, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza*".
- **metadati** di posta elettronica, come definiti dal Garante nel Provvedimento del 6 giugno 2024 - Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati: "*tali informazioni relative alle operazioni di invio e ricezione e smistamento dei messaggi possono comprendere gli*

indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell'instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, in relazione al sistema di gestione del servizio di posta elettronica utilizzato, anche l'oggetto del messaggio spedito o ricevuto"; I metadati **sono cancellati a 30 giorni dalla conclusione del rapporto di lavoro.**

- **log** di posta elettronica, che danno evidenza di data e ora dell'esecuzione di determinate operazioni da parte dell'utente (accesso, modifica, cancellazione e invio). I log **sono cancellati** a **30 giorni dalla conclusione del rapporto di lavoro.**

L'eventuale conservazione per un termine ancora più ampio potrà essere effettuata, solo in presenza di particolari condizioni che ne rendano necessaria l'estensione, comprovando adeguatamente, in applicazione del principio di accountability previsto dall'art. 5, par. 2, del GDPR.

4.4 Gestione operativa degli account di posta elettronica

- **Modalità di assegnazione del nome di posta elettronica**

1) Organi, Strutture ed articolazioni aziendali centrali e periferiche (PP.OO. DD.SS.SS.) Aree di gestione, Uffici di Staff: in questo caso, il formato dell'indirizzo di posta elettronica sarà composto da località.nomeuoc.eventualmenteattività@asp.rg.it (tale e-mail, poiché è condivisa, deve essere riconvertita dal SITD dell'ASP in cassette postali, in modo che gli utenti abilitati possano accedervi dal loro stesso account).
2) Personale dipendente/collaboratori/personale in presidio in servizio attivo: in questo caso, il formato dell'indirizzo di posta sarà nome.cognome@asp.rg.it. In caso di omonimia verrà aggiunto dopo il cognome l'anno di nascita su 2 cifre.

- **Criteri per la trasmissione dei dati personali presenti nei messaggi di posta elettronica**

1. È vietato l'uso dell'indirizzo e-mail in chiaro dei pazienti per l'invio agli stessi di comunicazioni provenienti dai reparti. L'invio di comunicazioni di carattere istituzionale su iniziative e attività promosse dall'ASP, le quali non contengono dati personali appartenenti a categorie particolari (dati sanitari, genetici, biometrici), è possibile solo verso i pazienti che hanno prestato previamente il proprio consenso all'uso della propria e-mail per tale finalità. In caso

di comunicazioni massive, l'e-mail dei pazienti destinatari deve essere inserita in copia conoscenza nascosta.

2. I dati sanitari dei pazienti possono essere condivisi dal personale sanitario, in presenza dei presupposti di liceità, tramite l'uso di piattaforme informatiche e/o di specifici canali approvati preventivamente dall'ASP. Qualora l'uso di e-mail aziendali per la condivisione di dati sanitari tra il personale sanitario e il paziente sia fondato sul consenso dello stesso (ad esempio per l'invio del referto on line), tale invio è ammissibile solo se il paziente ha prestato previamente il consenso. In ogni caso, i file allegati alle comunicazioni effettuate via e-mail, qualora contenenti dati sanitari dei pazienti, devono essere criptati e deve essere possibile aprirli solo tramite autenticazione da parte del destinatario.
3. Per le comunicazioni aziendali tra dipendenti, collaboratori e fornitori dell'ASP per motivi organizzativi e di gestione del lavoro, è possibile utilizzare l'e-mail personale o quella dell'ufficio anche in chiaro, a meno che non siano presenti nel testo o negli allegati dati personali di categorie particolari o giudiziari (di cui agli artt. 9 e 10 del GDPR) afferenti ai soggetti in indirizzario.
4. Ai fini del rispetto dello Statuto dei lavoratori, il SITD dell'ASP potrà fornire i log/file e testo della posta elettronica e delle attività eseguite tramite l'account del lavoratore solo ed esclusivamente su richiesta dell'autorità giudiziaria.

d) Allegati

Allegato 1 – privacy
Allegato 2 – reset
Allegato 3 – credenziali applicativi