Pravila prihvatljivog korištenja O365

Opće odredbe
Pravila prihvatljivog korištenja usluga Microsoft Office 365 (O365) koje pruža Sveučilište u Rijeci u skladu su sa Sigurnosnom politikom Sveučilišta, Pravilnikom o dodjeljivanju AAI@EduHr elektroničkih identiteta i informacijskom održavanju imenika AAI@EduHr elektroničkih identiteta Sveučilišta u Rijeci te Odlukom o prihvatljivom korištenju CARNet mreže . Korisnici O365-a dužni su se pridržavati ovih pravila.

Što je O365?
O365 je kratica za Office 365, pretplatničku uslugu temeljena na oblaku koja korisnicima pruža pristup nizu Microsoftovih aplikacija. O365 je dostupan u raznim planovima, od kojih svaki nudi različit skup značajki. Osnovni plan uključuje najvažnije aplikacije i usluge uključujući:

- Word: program za obradu teksta za stvaranje i uređivanje dokumenata.
- Excel: program za radne listove za stvaranje i upravljanje radnim listovima.
- PowerPoint: program za prezentacije za stvaranje i prezentiranje prezentacija.
- Outlook: klijent e-pošte za slanje i primanje e-pošte.
- OneDrive: usluga pohrane u oblaku za pohranu i dijeljenje datoteka.
- Teams: platforma za suradnju za čavrljanje, sastanke i dijeljenje datoteka.

O365 također uključuje niz drugih značajki, kao što su:

- skup alata za upravljanje mobilnim uređajima i aplikacijama.
- skup alata za sprječavanje gubitka povjerljivih podataka.
- skup alata za zaštitu podataka iz O365 od kibernetičkih napada.
- Integracija s drugima aplikacijama.

Cilj
Cilj ovih pravila je zaštititi sigurnost, privatnost i integritet podataka Sveučilišta u Rijeci i njezinih korisnika.

Primjena
Ova pravila primjenjuju se na sve korisnike O365-a, uključujući zaposlenike, studente, ugovorne partnere i druge osobe koje imaju pristup O365 resursima.

Pravila

Kompromitirani računi

Ako se utvrdi da je korisnički račun kompromitiran, račun će se blokirati. Kompromitirani račun je račun koji je vjerojatno pod kontrolom neovlaštenog korisnika. SIC (Sveučilišni informatički centar) će informirati korisnika i administratora imenika o blokiranom računu.

Kršitelji pravila

Korisnicama koji krše ova pravila korisnički račun bit će onemogućen, te korisnik morati kod administratora imenika (POPIS ADMINISTRATORA IMENIKA) zatražiti ponovo izdavanje lozinke. Svim kompromitiranim korisnicama uključit će se i višefaktorska autentifikaciju (MFA). MFA je dodatni sigurnosni sloj koji otežava neovlaštenim korisnicima pristup računu.

Praćenje korištenja

Sveučilište u Rijeci zadržava pravo praćenja korištenja O365-a kako bi osigurala da se poštuju ova pravila.

Izmjene

Sveučilište u Rijeci zadržava pravo izmjene ovih pravila u bilo kojem trenutku.

Kontakt informacije

Za više informacija o pravilima prihvatljivog korištenja O365, obratite se sic.podrska@uniri.hr.

Dodatne općenite informacije

Osim pravila navedenih u ovom pravilniku, korisnici O365-a trebaju biti svjesni i sljedećih općih sigurnosnih savjeta:

- Koristite jake lozinke i mijenjate ih redovito. Jaka lozinka je lozinka koja sadrži najmanje 12 znakova i koristi kombinaciju velikih i malih slova, brojeva i simbola.
- Budite oprezni kada klikate na linkove u e-pošti ili porukama. Ako niste sigurni je li link siguran, nemojte ga klikati.
- Instalirajte i ažurirajte antivirusni softver. Antivirusni softver pomaže u zaštiti računala od virusa, zlonamjernog softvera i drugih prijetnji.
- Redovito ažurirajte svoje softverske sustave. Ažuriranja softvera često uključuju sigurnosne zakrpe koje pomažu u zaštiti računala od prijetnji.