Универзитет у Београду
Институт за хемију, технологију и металургију
Институт од националног значаја за Републику Србију
Бр. 896
31.07. 2025 год.
Београд, Његошева 12

На основу члана 22. Статута Универзитета у Београду – Института за хемију, технологију и металургију – Института од националног значаја за Републику Србију, директор Института дана доноси:

ПРАВИЛНИК О УПОТРЕБИ ЕЛЕКТРОНСКЕ ПОШТЕ И ПОВЕЗАНИХ ДИГИТАЛНИХ АЛАТА на Универзитету у Београду – Институту за хемију, технологију и металургију – Институту од националног значаја за Републику Србију

I УВОДНЕ ОДРЕДБЕ

Члан 1.

Универзитет у Београду – Институт за хемију, технологију и металургију – Институт од националног значаја за Републику Србију (ИХТМ), посвећен је примени највиших стандарда у раду и дигиталној трансформацији, у складу са правним и етичким нормама. ИХТМ препознаје значај дигиталних алата за ефикасну комуникацију, безбедност и сарадњу, те овим Правилником даје смернице за професионално, безбедно и транспарентно коришћење институционалне електронске поште (е-пошта) и *Google Workspace* услуга.

Члан 2.

Овим Правилником се регулише коришћење електронске поште и *Google Workspace* алата са ИХТМ доменом од стране запослених у ИХТМ-у, бивших запослених и спољних сарадника.

Сви корисници су одговорни за сигурност својих налога, као и за правилно управљање и коришћење дигиталних алата у складу са важећим прописима и одредбама овог Правилника.

Непоштовање одредби Правилника може довести до дисциплинских мера у складу са интерним процедурама.

Правилник се примењује као допуна других прописа - Правилник о општим правилима приступа и коришћења услуга АМРЕС,[1] Кључни термини дефинисани су у **Додатку А**.

II КОРИШЋЕЊЕ ЕЛЕКТРОНСКЕ ПОШТЕ

Члан 3.

Налози за е-пошту се додељују искључиво за комуникацију везану за рад Института. Запослени који користе службени е-мејл налог Института треба да имају у виду да у електронској комуникацији представљају ИХТМ и да је свако службено обраћање

[1] https://www.amres.ac.rs/dokumenti/dokumenti/pravilnik_o_opstim_pravilima_i_koriscenju_usluga_amres.pdf

потенцијално део институционалне преписке. Очекује се да у својој комуникацији заступају интересе Института, уз поштовање професионалних стандарда и етике.

Службени е-мејл налози Института користе се искључиво за службену комуникацију. Употреба у приватне сврхе није дозвољена. Очекује се да запослени у електронској преписци поштују професионалне стандарде и да е-мејл користе у складу са интересима Института и радним обавезама.

Садржај електронске поште

Члан 4.

Поруке послате са ИХТМ домена морају бити у складу са академским и професионалним стандардима.

Садржај порука не сме садржавати увредљиве, дискриминаторне, провокативне изразе, нити материјале који крше ауторска права.

Члан 5.

Приликом коришћења е-поште није дозвољено следеће:

- Користити институционалну е-пошту за обављање личних финансијских трансакција (на пример, куповина или продаја робе, пренос новчаних средстава и др.)
- Слање масовних порука, укључујући спам и ланчане поруке (*chain emails*), које нису ауторизоване од стране надлежних администратора.
- Користити институционални налог за слање рекламних или промотивних материјала који нису директно повезани са службеним обавезама или интересима Института. Свака промоција мора бити у складу са интерним смерницама и добити одобрење од Администратора и Директора Института.

Стандарди електронске кореспонденције

Члан 6.

Корисници институционалне е-поште дужни су да, пре слања порука, провере исправност адреса примаоца како би се избегло ненамерно откривање поверљивих података и да на примљене поруке одговарају у разумном року, а без непотребног одлагања.

Препоручује се да се званична комуникација спроводи током радног времена, а поруке које нису хитне могу се унапред заказати коришћењем опције „*Schedule send*“ у *Gmail*-у.

У циљу повећања ефикасности комуникације, корисници требају да се уздрже од коришћења „*Reply all*“ опције за поруке у којима није неопходан одговор свим примаоцима.

Корисник налога је у обавези да врши редовно одржавање е-сандучета, укључујући архивирање или брисање застарелих порука.

Корисник налога је у обавези да приликом преноса великих датотека користи протокол за безбедно дељење фајлова. Под „протоколом за безбедно дељење фајлова” подразумевају се безбедне методе преноса као што су SFTP, FTPS или HTTPS (и сл.), који обезбеђују

заштиту података током дељења великих датотека и усклађени су са добрим информационим праксама.

Дељење приступних података, пренос приступа налогу или подешавање аутоматског прослеђивања, посебно ка адресама ван Института, није дозвољено.

Када корисник није доступан због годишњег одмора или продуженог одсуства, дужан је да подеси аутоматски одговор („*Out-of-Office*“) на свом е-налогу. Овај аутоматски одговор мора јасно навести период одсуства, као и алтернативни контакт у случају хитних ситуација, нарочито када се ради о осетљивим питањима. Препоручује се да се аутоматски одговор редовно ажурира како би информације биле тачне и актуелне.

Посебно одобрење за осетљиве комуникације

Члан 7.

Е-поруке које садрже поверљива документа, као и садржај који би могао да угрози пословну тајну Института, морају пре слања добити претходно писмено одобрење Директора ИХТМ.

Ова одредба обухвата, али није ограничена на:

- садржаји који су предмет патентне заштите;
- интерне развојне планове, финансијске податке, и документа о стратешким партнерствима;
- материјале у оквиру пројеката који имају клаузуле о поверљивости;
- фајлове чији садржај по својој природи захтева виши степен заштите и не може се безбедно пренети стандардним каналима.

Одобрења морају бити документована и архивирана ради потенцијалних ревизија.

III УПРАВЉАЊЕ НАЛОЗИМА

Креирање налога.

Члан 8

Налози за електронску пошту и приступ алатима *Google Workspace* са ИХТМ доменом додељују се запосленима у ИХТМ-у и спољним сарадницима по потреби.

Захтев за креирање или реактивацију налога подносе се Администраторима путем одговарајућег обрасца (**Додатак Б**). Након одобрења, налог ће бити креиран у року од два радна дана. Приступни подаци биће достављени кориснику на назначену е-мејл адресу приликом креирања налога.

Сваки налог је искључива одговорност регистрованог корисника, који је одговоран за све активности које се спроведу преко тог налога.

Корисници који захтевају помоћ приликом подешавања или опоравка налога, за помоћ се обраћају искључиво Администраторима.

Члан 9.

Сви званични институционални налози морају бити креирани у домену @ihtm.bg.ac.rs и настојати да следе формат:

ime.prezime@ihtm.bg.ac.rs

У случају да више корисника има исто име и презиме, Администратори ће креирати налог додавањем бројчаног суфикса или коришћењем друге униформне конвенције за обезбеђивање јединствености налога.

Налози који су отворени пре доношења овог Правилника, а који не испуњавају овај формат, остају непромењени, осим ако корисник сам не затражи измену.

Члан 10.

Спољним сарадницима, у сврху подршке њиховом раду и сарадњи са Институтом, могу бити додељени налози. За такве налоге, стално запослени у Институту који је одговоран за сарадњу мора попунити одговарајући образац (**Додатак В**) у име спољног сарадника, уз јасно навођење разлога за приступ и периода на који се налог захтева.

Е-Мејл налози по функцији

Члан 11.

Налози по функцији морају бити креирани по стандардним конвенцијама које укључују назив функције, како би јасно одражавали своју сврху.

Налози засновани на функцијама додељују се на основу одлуке Директора Института. Дељени приступ овим налозима је дозвољен, али сваки облик таквог распореда мора бити формално одобрен и документован од стране надлежних Администратора, као и јасно дефинисано која особа или особе носе одговорност за активности спроведене преко тог налога.

Актуелна, стално ажурирана листа свих *налоīа заснованих на функцијама* води се у **Додатку Г**. Администратори су дужни одмах ажурирати **Додатак Г** након сваког креирања, деактивације или измене структуре налога.

Члан 12

Службени налог ИХТМ-а је ihtm@ihtm.bg.ac.rs. Користи се за званичну комуникација између ИХТМ-а и институција или лица ван ИХТМ-а. Налогом управља Секретар ИХТМ-а и одговоран је за његово безбедно коришћење. Са тог налога се могу слати посебна обавештења или циркуларни мејлови дефинисаним групама или свим истраживачима или запосленима према потреби и у складу са садржајем е-мејла.

Члан 13.

Администратори заједнички користе е-мејл адресу admin@ihtm.bg.ac.rs за управљање е-мејл налозима и *Google Workspace*-ом. Корисници е-мејл налога и *Google Workspace*-а се администраторима обраћају путем наведене адресе.

Прекид, архивирање и приступ након престанка сарадње

Члан 14.

Након престанка радног односа запосленог, службени налог за е-пошту остаје активан у трајању од три месеца. Овај период служи искључиво за безбедно и одговорно преузимање службених комуникација и докумената од значаја за континуитет рада Института, уз поштовање професионалне етике и приватности.

За спољне сараднике, суспензија налога се спроводи истовремено са истеком важећег уговора или пројекта, уз примењивање истог периода од три месеца.

О престанку ангажовања запосленог у Институту, администраторе обавештава руководилац кадровске службе. О престанку ангажовања спољног сарадника, администраторе обавештава стално запослени у Институту који је одговоран за сарадњу.

Члан 15.

Уколико је потребан наставак приступа након званичног престанка сарадње, корисник подноси захтев за продужење приступа користећи одговарајући образац (**Додатак Б/В**). Уз Захтев неопходно је и приложити детаљно образложење и јасан временски оквир за продужење приступа. Продужење је могуће само уз писмено одобрење Директора ИХТМ и уз придржавање сигурносних протокола.

Члан 16.

Е-поруке и сви повезани подаци биће архивирани и чувани у периоду од 3 до 7 година, у складу са важећим законским прописима, регулативама програма финансирања (нпр. Horizon Europe, Фонд за науку), као и општеприхваћеним добрим праксама управљања подацима. Одговорност за безбедно управљање, контролу приступа и одлагање архивираних података имају овлашћени Администратори.

Члан 17.

По истеку периода од три месеца, неактивни налози ће бити званично деактивирани, осим ако није другачије договорено путем формалног захтева за продужење приступа.

Члан 18.

Када запосленом престане радни однос у Институту остваривањем права на пензију, одговарајући налог за електронску пошту остаје активан 12 месеци искључиво у циљу безбедног и одговорног преузимања службених комуникација и докумената од значаја за континуитет рада Института, уз поштовање професионалне етике и приватности. Процедура за продужење приступа пензионисаним особама је идентична оној која се примењује за све кориснике након престанка сарадње (**Додатак Б**).

Пренос и преусмеравање налога по функцијама

Члан 19.

Приликом промене вршиоца дужности или реорганизације унутар Института, *налози по функцијама* се преносе новим носиоцима. Све измене морају бити званично документоване и архивиране.

Одлуку о преносу доноси Директор Института.

При преносу налога, неопходно је попунити контролну листа за пренос налога (**Додатак Д**). Новом кориснику се достављају приступни подаци за налог, а измене се бележе у систему.

По завршеној примопредаји налога, неопходно је извршити ажурирање листе налога (**Додатак Г**).

IV СМЕРНИЦЕ ЗА КОРИШЋЕЊЕ GOOGLE WORKSPACE УСЛУГА

Општа упутства за коришћење *Google Workspace*-а

Члан 20.

ИХТМ званично користи *Google Workspace* као дигиталну платформу која обухвата алате попут *Gmail*-а, *Drive*-а, *Docs*-а, *Sheets*-а, *Slides*-а, *Forms*-а, *Calendar*-а, *Chat*-а, *Meet*-а и *Groups*-а за службену комуникацију, управљање документима, заказивање састанака и сарадњу.

Уколико корисници имају оправдане разлоге или специфичне потребе, дозвољено је коришћење и алтернативних дигиталних алата за сарадњу, уз услов да алати које се користе испуњавају исте или компатибилне безбедносне и интеграционе захтеве. Одлуку о дозволи за коришћење тих алата доносе Администратори.

Администратори ће пратити ажурирања и нове функционалности које *Google* објављује. Значајне измене које утичу на безбедност или радне токове биће одмах анализиране, а неопходне измене у Правилнику ће бити благовремено комунициране свим корисницима.

Спољним корисницима може бити дозвољен приступ у сврху састанака, сарадње или дељења фајлова, искључиво уз експлицитно одобрење. Сви захтеви за дељење морају осигурати да осетљиви подаци буду доступни само онима који имају потребна овлашћења.

Google групе и структурирана комуникација

Члан 21.

Google групе су дизајниране да олакшају интерну комуникацију, дистрибуцију обавештења, организацију информација и тимску координацију. Све групе, без обзира на сврху, користе се за директну службену комуникацију и дистрибуцију обавештења.

Институционалне групе, **запослени** (all@ihtm.bg.ac.rs), **истраживачи** (istrazivaci@ihtm.bg.ac.rs) и **администрација** (radna.zajednica@ihtm.bg.ac.rs) намењене су за дистрибуцију важних и званичних порука. Писма и обавештења која се шаљу овим

групама дозвољено је да објављује само именовано особље, а одговори и дискусије у овим групама су онемогућени. Институционалне групе формирају Администратори по налогу Директора и одговорни су за додељивање одговарајућих дозвола. Чланство у овим групама је обавезно за све кориснике.

Корисници налога су слободни да креирају додатне групе на основу специфичних оперативних потреба, тимова или пројеката, уз поштовање општих смерница за именовање и приступ.

Комуникација у реалном времену – *Google Calendar, Chat* и *Meet*

Члан 22.

Препоручује се да се сви састанци и службени догађаји заказују преко *Google Calendar*-а, уз детаљне описе и контролисане поставке за дељење информација.

Комуникација у реалном времену путем *Google Chat*-а и састанци на *Google Meet*-у морају бити вођени професионално. За састанке који укључују спољна лица (нпр. за пројекте или сарадњу), позивнице се шаљу искључиво неопходним (овлашћеним) лицима.

Уколико се састанци снимају, снимци се чувају на безбедном месту, а како је дефинисано Правилником о управљању документима. Снимање састанака дозвољено је само уз сагласност свих учесника.

V БЕЗБЕДНОСТ И ЗАШТИТА ПОДАТАКА

Члан 23.

Корисници налога су у обавези да користе јединствене лозинке које се редовно мењају (најмање једном годишње) и да омогуће двофакторску аутентификацију, где год је то могуће.

Корисник је дужан да све приступне податке чува као строго поверљиве.

При приступу институционалној е-пошти и *Google Workspace* алатима, укључујући и приступ мобилним уређајима или путем удаљеног приступа, такви уређаји морају имати ажуриран оперативни систем, ажуриран антивирусни софтвер и безбедне мрежне поставке. Уређаји који не испуњавају наведене услове могу имати ограничен приступ или неспецифичне потешкоће у приступу институционалним сервисима.

Члан 24.

Само типови фајлова одобрени од стране Института – како је наведено у **Додатку Ђ** – могу се делити путем е-поште или путем *Google Workspace* алата. Било који фајл који није изричито наведен захтева претходно одобрење Администратора пре дељења.

При приступу *Google Workspace* сервисима, корисници су дужни да примењују уграђене контроле верзија како би се пратила детаљна историја измена, чиме се обезбеђује транспарентност и могућа ревизија.

Уз стандардну SSL/TLS заштиту коју пружа *Google Workspace*, препоручује се разматрање додатних метода енкрипције (нпр. S/MIME или PGP) за веома осетљиве комуникације.

Корисници налога су у обавези да приликом отварања прилога и линкова, претходно провере идентитет пошиљаоца како би се избегли ризици од *phishing* напада и инфекција злонамерним софтвером (*malware*).

Члан 25.

Приступ дигиталним ресурсима додељује се искључиво у складу са *принципом најмање потребе за приступом* (**прилог А**). Овај принцип важи за сваку апликацију *Google Workspace*-а, а детаљни услови (као што су прописане дозволе, безбедносни захтеви и политика приступа) редовно се ревидирају. При ревизији, морају бити јасно документовани одговорности свих укључених страна.

Свако одступање од стандардних дозвола или привремено повећање права (нпр. привремено подизање права за објављивање) мора бити документовано и писмено одобрено од стране надлежних администратора.

Корисници налога треба да одговорно рукују осетљивим подацима, осигуравајући да су доступни само овлашћеном особљу. Неовлашћено дељење или неисправно руковање подацима строго је забрањено.

V НАДЗОР, РЕВИЗИЈА, ИНЦИДЕНТИ

Надзор

Члан 26.

Институт примењује аутоматизоване алате за снимање логова и алармирање како би пратио значајне аномалије у окружењу *Google Workspace*-а и е-мејлова. Ови алати означавају високо приоритетне проблеме, као што су необични обрасци приступа, понављајући неуспешни покушаји пријаве или сумњиве активности које могу указивати на *phishing* инциденте.

Периодично, на бази процене ризика, врши се ревизија (шестомесечно) ради прегледа логова приступа, дозвола за дељење и активности унутар група. Циљ ревизија је да се осигура да:

- Сви активни налози остану правилно оправдани и обезбеђени.
- Привремена или након прекида сарадње приступна права буду документована и адекватно ограничена.
- Дозволе за дељење фајлова и фолдера поштују *принцип најмање потребе* (**прилог А**).

Реаговање на инциденте

Члан 27.

Било који сумњив прекршај, неовлашћени приступ, *phishing* покушај, злоупотреба налога или други безбедносни инцидент мора се одмах пријавити једном од именованих Администратора (**Прилог Е**).

Након пријема извештаја о инциденту, примењују се следећи нивои ескалације:

- Ниво 1 – Почетни одговор: администратор прегледава инцидент коришћењем аутоматизованих логова и предузима почетне корективне мере (нпр. ресет лозинки, блокирање налога или мала конфигурациона подешавања).
- Ниво 2 – Секундарна ескалација:
  Ако почетни одговор не реши инцидент, администратори заједно процењују ситуацију и ескалирају проблем – укључивање колегијума и руководиоца правних, кадровских и административних послова, и по потреби руководиоце центара или других организационих јединица.
- Ниво 3 – Спољна ескалација:
  За озбиљне инциденте који се не могу решити интерно (на пример, упорни прекршаји или напредни сајбер напад), администратори ће ангажовати спољашњу подршку, контактирајући организације као што су AMRES (Академска мрежа Србије) или RCUB (Рачунарски центар Универзитета у Београду).

Све предузете мере и исходи морају бити детаљно документовани у пост-инцидентном извештају, који укључује закључке и неопходне измене у процедурама надзора и реаговања.

Члан 28.

У случају хардверских проблема, техничка подршка ће реаговати како би се минимизирао прекид рада, спроводећи систематичну интервенцију и ескалацију уколико је то потребно.

Након пријема проблема, примењују се следећи нивои ескалације:

- Ниво 1 – Основна техничка подршка
  Техничко особље пружа иницијалну помоћ за идентификацију и решавање хардверских проблема (на пример, поправка компјутера, ажурирање периферних уређаја, провера физичке опреме). Уколико проблем није одмах решен, инцидент се ескалира.
- Ниво 2 – Ескалација ка администраторима
  Ако проблем остаје нерешен након интервенције на нивоу 1, техничко особље ескалира инцидент администраторима, који детаљно процењују ситуацију и предузимају додатне мере. Овим корацима се покривају критични хардверски проблеми који могу утицати на скуп њихових дигиталних услуга.
- Ниво 3 – Спољна ескалација
  За озбиљне, или сложене хардверске инциденте који се не могу интерно решити, администратори ће ангажовати спољашње сервисне партнере или техничке центре (на пример, администраторе ХемНет-а или ТМФ-а, сервисни центар или регионални технички центар). Сви кораци спољашње ескалације морају бити адекватно документовани.

Сви кораци ескалације и предузете мере у случају хардверских инцидената морају бити детаљно документовани у пост-инцидентном извештају. Овај извештај треба да садржи закључке, препоруке за будуће измене и мере за побољшање процедуре одговора на хардверске проблеме.

VI АДМИНИСТРАТИВНЕ УЛОГЕ И ОДГОВОРНОСТИ

Члан 29.

Директор Институт-а именује:

- Два администратора одговорна за управљање системима е-поште и *Google Workspace*-а. Они су главни контакт за све проблеме везане за дигиталне сервисе, безбедност налога, надзор приступа, осигуравају континуитет и интегритет сервиса, и сарађују са спољашњом подршком (AMRES/RCUB) када је то потребно.
- Две особе специјализоване за техничку и хардверску подршку, одговорне за одржавање и поправке рачунарске опреме, решавање хардверских инцидената и пружање директне подршке корисницима у вези са хардверским проблемима.

Члан 30.

Администратори су одговорни за:

- Обраду захтева за налоге у складу са Секцијом III, коришћењем званичних образаца, и осигуравање да су све измене (отварање, деактивација итд.) одмах евидентиране у **Прилогу Г**.
- Надзор над процедурама задржавања и архивирања података како би се осигурала усклађеност са смерницама о заштити података.
- Документацију сваког привременог повећања дозвола или изузетка кроз утврђени систем захтева за измене.
- Надгледају аутоматизоване аларме и прегледају извештаје о инцидентима.
- Иницирају процес реаговања на инциденте како је дефинисано у Члану 27 и управљају решењем нивоа 1. Сарађују са управом (за ескалацију на ниво 2 када је потребно. Ангажују спољашњу подршку ако интерно решење инцидента није довољно. Сви кораци ескалације, укључујући донете одлуке и предузете мере, морају бити детаљно документовани и комуницирани релевантним странама.
- Одржавају и редовно ажурирају детаљну документацију о свим процедурама везаним за управљање налогом, реаговање на инциденте и конфигурацију система.
- Периодично ревидирају и ажурирају административне процедуре како би се интегрисале најбоље праксе и адресирале безбедносне претње.
- Обавештавају све кориснике о значајним изменама у процедурама или системима, осигуравајући да су упутства и материјали за обуку доступни.
- Администратори су дужни да осигурају поверљивост свих интерних и осетљивих података, као део својих одговорности за безбедност информација.

- Администратори обављају своје послове уз коришћење налога admin@ihtm.bg.ac.rs, који служи као централна адреса за интерну комуникацију и координацију активности везаних за систем и информациону безбедност.

Члан 31.

Техничка и хардверска подршка је одговорна за:

- Обављање почетне интервенције и решавање проблема везаних за хардвер (на пример, одржавање рачунара, периферних уређаја, серверске опреме и мрежне инфраструктуре).
- Успостављање првог нивоа подршке за све хардверске инциденте.
- Ескалација проблема администрацији уколико проблем није могуће локално решити, према процедури дефинисаној у члану 28.

VII УСАГЛАШЕНОСТ, СПРОВОЂЕЊЕ, САНКЦИЈЕ

Члан 32.

Сви корисници е-поште и *Google Workspace*-а са ИХТМ доменом дужни су да се придржавају овог Правилника. Усаглашеност се надгледа од стране именованих Администратора у сарадњи са управом Института. Сви корисници морају поштовати утврђене смернице, а било каква одступања морају бити документована или пријављена.

Члан 33.

Администратори су одговорни да прегледају свако кршење и предузму одговарајуће корективне мере; документују све прекршаје и инциденте, укључујући детаље прекршаја, мере решења и поправне активности; одмах пријаве сумњиве ситуације како би се спречиле додатне последице.

Члан 34.

Прекршаји овог Правилника могу довести до санкција, које укључују, али нису ограничене на:

- Писмена упозорења;
- Привремену суспензију приступа е-пошти и другим ресурсима, у случајевима озбиљних или поновљених прекршаја, уз претходну процену утицаја на текуће службене обавезе;
- Повлачење приступних права, уколико постоји јасан ризик по безбедност система или интегритет институционалне комуникације;
- Упућивање на дисциплинске или законске процедуре у складу са интерним прописима Института.

Тежина санкција зависи од природе и утицаја прекршаја, а санкције ће се доследно примењивати у оквиру дисциплинарног система Института.

VIII ПРЕГЛЕД, ИЗМЕНЕ, АЖУРИРАЊЕ ПРАВИЛНИКА

Члан 35.

Овај Правилник ће бити периодично прегледан како би се осигурала његова актуелност у складу са технолошким напрецима, регулаторним изменама и потребама. Преглед ће се вршити најмање једном годишње, или чешће ако дође до значајних промена.

Члан 36.

Измене Правилника могу иницирати Администратори, чланови Колегијума Института или други запослени, путем писаних предлога достављених Администраторима. Све предложене измене морају бити детаљно документоване и размотрене у консултацији са Колегијумом. Финализација измена захтева званично одобрење директора Института.

Све измене ће бити објављене путем званичних канала, а ажурирана копија Правилника ће бити доступна свим заинтересованим странама.

Члан 37.

Сви корисници су дужни да се упознају са најновијом верзијом овог Правилника.

За подршку у коришћењу функционалности *Google Workspace*-а, корисници се подстичу да консултују званичне ресурсе (нпр. *Google Workspace for Education Help Center*[2]).

VIII ЗАКЉУЧНЕ ОДРЕДБЕ

Члан 38.

Сви прилози (**Прилози А** до **Е**) представљају интегрални део овог Правилника.

Правилник ступа на снагу од дана објављивања на интернет страни ИХТМ-а и остаје на снази све док га Институт не измени или поништи.

ИХТМ

Директор проф. др Јасмина Стевановић

[2] https://workspace.google.com/education/

ЛИСТА ПРИЛОГА

Прилог А – Дефиниције

Овај прилог садржи дефиниције кључних термина који се користе у овом Правилнику и представља основ за разумевање свих одредби.

- **Налог**
  Јединствени идентификовани електронски налог који се додељује запосленима, лицима којима је радни однос у Институту престао остваривањем права на пензију, истраживачима или спољним сарадницима, и који омогућава приступ институционалним дигиталним алатима (електронској пошти и *Google Workspace* сервисима).
- **Корисник**
  Лице које користи званични налог за приступ дигиталним алатима Института. Ово укључује запослене, лица којима је радни однос у Институту престао остваривањем права на пензију, истраживаче, као и спољне сараднике који сарађују са Институтом, а како је дефинисано овим Правилником.
- **Администратори**
  Особе именоване од стране Института, а које су одговорне за управљање системима е-поште и *Google Workspace*-ом, надзор приступних права, спровођење безбедносних мера и за документацију свих измена у систему.
- **Принцип најмање потребе**
  Безбедносни концепт који подразумева да корисници, процеси или системи имају приступ само онима ресурсима и информацијама који су неопходни за обављање њихових конкретних задатака или функција. Овај приступ служи као превентивна мера за смањење ризика од злоупотребе, неовлашћеног приступа или случајних грешака које могу довести до компромитовања података. Примена принципа најмање потребе укључује: ограничен приступ (корисници добијају приступ само специфичним ресурсима, базама података или системима који су потребни за њихове радне задатке); дозволе за дељење (свим дозволама за приступ и дељење информација се пажљиво управља, а свака промена у правима се документује); редовна ревизија (права приступа се периодично преиспитују како би се осигурало да се не додељују превелике или непотребне привилегије).
- **Безбедносни инцидент**
  Догађај или низ активности за које постоји разлог сумње да могу угрозити интегритет, поверење или рад дигиталних услуга Института, укључујући злоупотребе, нападе *phishing* или софтверске неисправности.
- **Ескалација**
  Процедура повећања нивоа реаговања и укључивања додатних ресурса у случају да иницијална интервенција не доведе до решења инцидента. Ово укључује постепено ангажовање надређених органа или спољашњих сервиса у зависности од озбиљности проблема.
- **Службена комуникација**
  Електронска порука послата са званичног институционалног налога, која представља службено информисање, интерну комуникацију и интерне радне

процесе Института. Сваки садржај слања се сматра службеном информацијом од значаја за рад Института.

- **Хардверска подршка**
  Особе именоване од стране Института, које су специјализоване за одржавање, поправке и решавање инцидента везаних за хардвер. Оне представљају први контакт за све хардверске проблеме, а уколико је потребно, ескалирају инцидент надлежним администраторским јединицама.
- **Дигитални алати**
  Апликације и платформи које омогућавају електронску комуникацију, управљање документима, сарадњу и друге услуге. Ови алати омогућавају већину свакодневних операција у области службене комуникације обухватају, али нису ограничени на, сервисе попут Gmail-a, Google Drive-a, Docs-a, Sheets-a, Slides-a, Forms-a, Calendar-a, Chat-a, Meet-a и Groups-a.
  Gmail: Основна апликација за електронску пошту која пружа безбедан и поуздан канал за службену комуникацију. Корисници могу да шаљу, примају и архивирају поруке, користе филтере за организовање сандучета и приступају могућностима попут слања одложених порука („*Schedule send*“) и интегрисане претраге.
  Google Drive: *Cloud* складиште за чување, дељење и сарадњу. Омогућава приступ фајловима са било ког уређаја, осигуравајући да се документи аутоматски синхронизују и безбедно чувају.
  Google Docs: Апликација за креирање и уређивање текстуалних докумената, која омогућава да више корисника истовремено раде на истом документу. Подржава коментаре, предлоге измена и ревизије, што олакшава тимску сарадњу.
  Google Sheets: Апликација за креирање и уређивање табела и прегледа података. Пружа могућности филтрирања, графикона и анализа података и тимску сарадњу.
  Google Slides: Апликација за креирање презентација која омогућава додавање текстова, слика, видео записа и анимација, те сарадњу више корисника у стварном времену.
  Google Forms: Алат за креирање онлајн образаца, анкета и тестова, који олакшава прикупљање повратних информација или сарадњу током интерних истраживања.
  Google Calendar: Апликација за планирање и заказивање састанака, која омогућава корисницима да координишу обавезе, креирају подсећања и управљају распоредом током дана.
  Google Chat: Услуга за онлајн размену порука и групне дискусије, која олакшава комуникацију у реалном времену са члановима тима или одељења, а интегрисана је са осталим Google Workspace алатима.
  Google Meet: Алат за видео састанке и конференције који омогућава виртуелне састанке, вебинаре и презентације. Подржава дељење екрана, чиме се побољшава сарадња на даљину.
  Google Groups: Платформа за формирање група и форума у који се могу укључити веће групе корисника. Омогућава једноставно дељење информација, расподелу обавештења, и организовање тимова или пројеката у оквиру институције.

Прилог Б – Образац за отварање налога за запослене

Овај образац служи за формално подношење захтева за креирање, реактивацију, или измену институционалних е-налога, укључујући и налоге засноване на функцијама.

Основни подаци:

- **Име и презиме:** _____
- **Центар / организациона јединица:** _____
- **Звање / радно место:**
- **Контакт информације:**
  - **Е-мејл адреса:** _____
  - **Телефон:** _____
  - **(опционално) Адреса:** _____

Захтев:

- **Тип налога:**
  [ ] Редовни налог
  [ ] Налог заснован на функцији
- **Врста захтева:**
  [ ] Креирање
  [ ] Реактивација
  [ ] Измена
  [ ] Продужетак приступа

- **Разлог (опис):**

- **Специфични захтеви или напомене (ако постоје):**

Одобрење:

- **Потпис непосредног руководиоца:** _____
- **Датум:** _____

Напомене:

- Попуњавањем и потписивањем овог обрасца, корисник потврђује да је упознат са условима коришћења институционалних налога и да ће поштовати прописане процедуре описане у Правилнику.
- Образац је обавезан за све захтеве везане за институционалну е-пошту и налоге, те се шаље администраторима за даљу обраду.

Прилог В – Образац за отварање налога за спољне сараднике

Овај образац служи за формално подношење захтева за креирање, реактивацију, или измену институционалних е-налога за спољног сарадника.

Основни подаци спољног сарадника:

- **Име и презиме:** _____
- **Организација/Институција:** _____
- **Контакт информације:**
  - **Е-мејл адреса:** _____
  - **Телефон:** _____
  - **(опционално) Адреса:** _____

2. Захтев за налог:

- **Тип налога:**
  [ ] Редовни налог
- **Разлог захтева:**

(опишите службени разлог за приступ – на пример, подршка пројекту, сарадња са Институтом итд.)

3. Период приступа:

- **Почетак: /**/_____ *(дан/месец/година)*
- **Завршетак: /**/_____ *(дан/месец/година)*

4. Одобрење:

- **Име и презиме запосленог одговорног за сарадњу:** _____
- **Центар:** _____
- **Потпис непосредног руководиоца:** _____
- **Датум: /**/_____

Напомене:

- Попуњавањем овог обрасца, запослени који је одговоран за сарадњу потврђује да су сви достављени подаци тачни и да је захтев оправдан.
- Образац се шаље надлежном администратору ради даљег процесирања и креирања налога.
- Сви захтеви се документују и ревидирају у складу са интерним прописима Института.

Прилог Г – Листа Налога по функцији

Ова листа се редовно ажурира како би одговарала променама у организационој структури и потребама пројектних тимова. Администратори воде интерну листу у форми:

Назив	E-mail	Функција	Опис/сврха	Имена и презимена одговорних лица	Датуми креирања /гашења	Статус (активан/неактиван)
	...@ihtm.bg.ac.rs					

Тренутно активни налози:

Назив налога	E-mail	Функција/одговорност
Службени налог ИХТМ-а	ihtm@ihtm.bg.ac.rs	Секретар ИХТМ-а
Директор ИХТМ-а	direktor@ihtm.bg.ac.rs	Директор ИХТМ-а
Администратори	admin@ihtm.bg.ac.rs	Администратори
IT подршка	itpodrska@ihtm.bg.ac.rs	IT администратори
Колегијум	kolegijum@ihtm.bg.ac.rs	Колегијум
Тело за трансфер технологија	transfer.tehnologija@ihtm.bg.ac.rs	Тело за трансфер технологија
Канцеларија за пројекте и међународну сарадњу (ICPO)	icpo@ihtm.bg.ac.rs	Запослени у Канцеларији за пројекте и међународну сарадњу
Службени налог институционалног репозиторијума	cer-info@ihtm.bg.ac.rs	Администратори репозиторијума
Акредитована лабораторија ЦХ– извршни руководилац	izvrsni.chlab@ihtm.bg.ac.rs	Извршни руководилац акредитоване лабораторије ЦХ
Акредитована лабораторија ЦХ– технички руководилац	tehnicki.chlab@ihtm.bg.ac.rs	Технички руководилац акредитоване лабораторије ЦХ
Акредитована лабораторија ЦХ– квалитет	kvalitet.chlab@ihtm.bg.ac.rs	Особа задужена за квалитет у акредитованој лабораторији ЦХ
Безбедност	bezbednost@ihtm.bg.ac.rs	Одговорно лице за безбедност
Фактуре	fakture@ihtm.bg.ac.rs	Одговорно лице за фактурисање
Шеф рачуноводства	finansije@ihtm.bg.ac.rs	Шеф рачуноводства
ИХТМ - набавке	javne.nabavke@ihtm.bg.ac.rs	Служба јавних набавки
Наруџбенице	narudzbenice@ihtm.bg.ac.rs	Служба јавних набавки
Научно веће	nv@ihtm.bg.ac.rs	Председник научног већа
Центар за екологију и техноекономику	cete@ihtm.bg.ac.rs	Руководилац центра
Центар за хемију	depchem@ihtm.bg.ac.rs	Руководилац центра

Назив налога	E-mail	Функција/одговорност
Центар за материјале и металургију	cmm@ihtm.bg.ac.rs	Руководилац центра
Центар за електрохемију	ceh@ihtm.bg.ac.rs	Руководилац центра
Центар за екологију и техноекономику	cete@ihtm.bg.ac.rs	Руководилац центра
Центар за катализу и хемијско инжењерство	ckhi@ihtm.bg.ac.rs	Руководилац центра
Центар за микроелектронске технологије	cmt@ihtm.bg.ac.rs	Руководилац центра
Центар изврсности за хемију и инжењеринг животне средине	civ.hzs@ihtm.bg.ac.rs	Руководилац центра изврсности
Синдикат науке ИХТМ	sindikat@ihtm.bg.ac.rs	Председник синдиката науке ИХТМ
Интерна конференција ИХТМ	korakuiskorak@ihtm.bg.ac.rs	Председник организационог одбора конференције
Odbor za rodnu ravnopravnost	gender.equality@ihtm.bg.ac.rs	Odbor za rodnu ravnopravnost: Ivana Dimitrijević, Tanja Šolević Knudsen, Miloš Ćirić

Прилог Д – Контролна листа за пренос налога

Ова листа представља низ корака које одговорна лица морају следити и документовати, како би се осигурао потпуно преношење свих релевантних података и приступних права.

Основни подаци

- **Власник налога (особа која преноси налог):**
  Име и презиме: _____
  Функција: _____
- **Нови власник налога (особа која преузима налог):**
  Име и презиме: _____
- **Датум преноса: /**/_____ *(дан/месец/година)*

Кораци за пренос

1. **Идентификација налога:**
   - Проверити да ли је налог ажуран и документовати све релевантне податке (корисничко име, додељене улоге).
   - Потврдити списак дигиталних ресурса који су повезани са налогом (Gmail, Google Drive, Docs, Sheets итд.).
2. **Архивирање и пренос података:**
   - Архивирати све важне е-поруке, фајлове и базе података које су критичне за рад.
   - Преузети или форматирати податке ако је потребно, како би нови власник био у могућности да настави са коришћењем без губитка информација.
3. **Прекидање привременог приступа:**
   - Проверити и документовати све привремене приступне листе или дозволе које су додељене, а које је потребно по потреби уклонити или пренети новом власнику.
   - Осигурати да примена безбедносних мера (пр. промена лозинке, ажурирање аутентификационих података) задржи компатибилност са интерним прописима.
4. **Преглед и потврда:**
   - Администратори проверавају да су сви кораци успешно извршени.
   - Новом и старом власнику налога се потврђује да су сви релевантни документи и подаци пренети, те да је налог спреман за наставак употребе.
5. **Финална документација и потпис:**
   - Обавезно попунити контролну листу уз напомене свих корака и измена.
   - Потписати Контролну листу како би се потврдило да је процес преноса завршен у складу са прописима.

Пример табеле за контролну листу

Корак	Опис активности	Одговорно лице	Потпис и датум
1	Идентификација налога и провера релевантних података		_____
2	Архивирање и пренос свих важних докумената и е-порука	Власник налога	_____
3	Преглед и ажурирање привремених приступних права	Администратор	_____
4	Преглед и потврда преноса		_____
5	Финална документација: попуна контролне листе и финални потписи	Власник и нови власник	_____

Напомене:

- Сваки корак мора бити документован, а контролна листа задржана као део интерне евиденције.
- Уколико дође до било каквих одступања у току процеса, надлежна лица морају донети додатне мере у складу са безбедносним прописима.
- Контролна листа треба да буде доступна за будуће ревизије и анализе.

Прилог Ђ – Дозвољени типови фајлова за дељење

Путем институционалне е-поште или Google Drive-а не смеју се слати .exe документи

Врсте фајлова које су дозвољене за дељење путем институционалне е-поште или Google Drive-а:

Документи:

- .doc / .docx (Microsoft Word)
- .pdf (Adobe Acrobat)
- .txt (обичан текст)
- .odt (OpenDocument Text)

Табеле:

- .xls / .xlsx (Microsoft Excel)
- .csv (Comma-Separated Values)
- .ods (OpenDocument Spreadsheet)

Презентације:

- .ppt / .pptx (Microsoft PowerPoint)
- .odp (OpenDocument Presentation)

Мултимедијални фајлови:

- .jpg / .jpeg / .png / .tif (слике)
- .svg / .eps (векторске слике)
- .mp4 (видео фајлови)

Компримовани фајлови:

- .zip
- .rar

Програмски фајлови (само уз одобрење Администратора):

- .py (Python скрипте)
- .c / .cpp
- .m (MATLAB скрипте)
- java
- .tex /.bib (LaTeX)
- .R (R скрипте)
- .json

Фајлови везани за хемију и структурне податке:

- .cif (Crystallographic Information File)
- .pdb (Protein Data Bank формат)
- .xyz (атомске координате и молекуларне структуре)
- .sk2 (ChemSketch формат) и формати генерисани експортом из овог програма
- .cdx (Chem Draw формат) и формати генерисани експортом из овог програма

- .skc и .rxn (ISIS Sketch формат) и формати генерисани експортом из овог програма
- .mol (MDL Molfile формат)

Технички и инжењерски фајлови:

- .dwg / .dxf (формати за CAD цртеже, ако је потребно за пројектну документацију или дизајн лабораторијске опреме)
- .opju / .opj (OriginLab)
- .pzfx / .pzf (GraphPad Prism)

Ревизија овог прилога се врши периодично и списак се ажурира како би одговарао технолошким и оперативним потребама.

Прилог Е – Процедуре за решавање инцидента

Циљ

Ове процедуре имају за циљ да обезбеде брзу и ефикасну идентификацију, пријављивање и решавање сигурносних и оперативних инцидената, с тим да се минимизирају потенцијалне штете по информациони систем и да се одржи континуиран рад критичних сервиса.

Дефиниције

- **Безбедносни инцидент**: Сваки догађај или низ активности за које постоји разлог сумње да могу угрозити интегритет, поверљивост или доступност дигиталних ресурса Института.
- **Инцидент**: Догађај који одступа од нормалног рада, укључујући, али не ограничавајући се на, покушаје неовлашћеног приступа, *phishing* нападе, софтверске неисправности и поремећаје у систему.

Процедуре за извештавање

- **Непосредно пријављивање**
  - Сви корисници који забележе сумњиве активности (нпр. повећани број неуспешних покушаја пријаве, необјашњене приступе, упозорења система) морају одмах обавестити надлежне администраторе путем званичних комуникационих канала (електронском поштом или телефоном).
- **Формални извештај**
  - Попуњава се формулар за пријављивање инцидента, у коме се детаљно описује врста инцидента, време и датум појаве, предузете кораке (ако их има) и контакт информације лица које пријављује инцидент.
- **Документација**
  - Сви извештаји се чувају као део пост-инцидентне документације, која ће бити предмет ревизије и анализе с циљем побољшања постојећих процедура.

Процедуре за решавање инцидента

a. **Првобитна процена**
   - Надлежни администратори брзо процењују инцидент у складу са утврђеним критеријумима (ниво: низак, средњи, висок) и приступају првобитној интервенцији (нпр. ресет лозинки, блокирање приступа).
b. **Интервенција**
   - Ако инцидент захтева додатне мере, покреће се ескалација (члан 26 Правилника)
   - Прихватају се кораци за уклањање претње, поправку система и поновну проверу функционалности.
c. **Пост-инцидентна анализа**

- Након решавања инцидента, врши се детаљна анализа, која укључује креирање пост-инцидентног извештаја са описом догађаја, предузетим мерама и препорукама за побољшање процена и спречавање будућих инцидената.

Одговорности

- **Корисници**: Дужни су да одмах пријаве све сумњиве активности.
- **Администратори**: Редовно прате системске логове, остварују почетне мере реаговања и обезбеђују да се сви кораци документују.
- **Колегијум**: Анализира озбиљне инциденте, одлучује о ескалацији и спроводи одговарајуће интервенције.