Политика за използване на ИТ ресурсите

Съдържание

Информация за документа

URL на документа: https://orgchm.sharepoint.com/sites/allcompany

Код на документа: ITP-04
Версия на документа: 1.0
Одобрена от: директора на ИОХЦФ
Дата на одобрение: 17.01.2022 г.
Дата на публикуване: 17.01.2022 г.
Дата на последен преглед: 15.12.2021 г.
Контакт за връзка и обмен на информация: IT.Services@orgchm.bas.bg
Разработен от звеното за ИТ услуги (Антон Ангелов, Георги Гергинов, Владимир Димитров, Светлана Симова)

1. Въведение

1.1 Тази политика е част от политиките за използване на ИТ в ИОХЦФ и определя правилата и отговорностите на потребителите при използването на ИТ ресурсите на ИОХЦФ;

1.2. Всички потребители, които достъпват и използват информационните ресурси на ИОХЦФ следва да прилагат тази политика, политиката за информационна сигурност и всички други изисквания, описани в пакета от документи "Политики и ръководства за използване на ИТ в ИОХЦФ";

2. Цели

2.1. Тази политика представлява стремеж да се намери баланс между потребностите, породени от функциите на Института (като продуктивност и оперативност) и изискванията за сигурността;

2.2. Всички служители от и извън ИОХЦФ имат етично и морално задължение да защитават вътрешната информация, притежавана или съхранявана от Института, както и да поддържат поверителността на тази вътрешна информация;

2.3. Политиката споделя изцяло принципите за академичната свобода, като заедно с това, ИТ ресурсите на ИОХЦФ следва да се използват отговорно и да не злепоставят или нарушават репутацията на института по никакъв начин. По-специално политиката за използване на ИТ ресурсите на ИОХЦФ е насочена към:

1) Регламентиране на физическия достъп до оборудване, компютри на ИОХЦФ с управление на пароли, периферии, комуникационно оборудване, информация;
2) Защита на операционните системи и сигурност на програмите, включително регламентиране на достъпа до компютърната мрежа, защита чрез антивирусни програми, управление на профила и на паролите на потребителите;
3) Правилно използване на оборудването и техниката на ИОХЦФ - възпроизвеждане, изменение и разпространение на информацията;
4) Процедури за превенция и възстановяване при повреда за предотвратяване на загуби на информация при форсмажорни обстоятелства или кражби/умисъл, включително в случаите на извършване на компютърни операции с много потребители;
5) Управление на всички активи свързани с Информационните технологии (ИТ) и докладване при инциденти;

2.4. Политиката трябва да гарантира, че са взети всички разумни мерки за предпазване на ИОХЦФ и електронната информация от загуби, неразрешен достъп или разкриване на служебна тайна.

3. Обхват

3.1 За целите на настоящия документ ИОХЦФ се дефинира като организация, която включва научен персонал и научно-помощен персонал, административно обединен в лаборатории, администрация и помощен персонал, както и определен брой обучаващи се и наематели.

3.2 Тази политика се прилага за всички служители на ИОХЦФ, студенти, аспиранти, гости, партньори, временни посетители, наематели и всички други, които използват информационните ресурси на ИОХЦФ, за които ще използваме общото понятие "потребители". Политиката се прилага независимо от начина, по който се достъпват тези ресурси (локално или отдалечено).

3.3 Информационните ресурси на ИОХЦФ включват:

- Информацията, която се събира, обработва и съхранява от ИОХЦФ по електронен път;
- ИТ ресурсите на ИОХЦФ (OrgChmNet), чрез които информацията се събира, обработва и съхранява.

3.4 ИТ ресурсите на ИОХЦФ обединяват всички технологични средства за събиране, обработване и съхраняване на информацията. Основни компоненти са:

- сървърно компютърно оборудване (хардуер и софтуер), сървърни помещения;
- комуникационни мрежи (хардуер и софтуер);
- всички крайни клиентски устройства (като десктоп компютри, лаптопи, таблети, работни станции, апарати, мобилни устройства), които са свързвани към OrgChmNet;
- Всички периферни устройства, които са включени в OrgChmNet (принтери, скенери и др.);
- всички ИТ услуги, които се предоставят от ИТ инфраструктурата на ИОХЦФ (като файлови услуги, услуги за печат, електронна поща, услуги за отдалечен достъп и т.н.).

3.5. ИТ ресурсите на ИОХЦФ могат да се достъпват чрез крайни устройства, които са притежание на института, както и от устройства, които са собственост на потребителите (Bring Your Own Device - BYOD). Политиката се прилага независимо чрез какъв вид устройства се достъпват и използват ИТ ресурсите на ИОХЦФ. Изискванията за всички крайни устройства, чрез които се достъпват и използват ресурсите на ИОХЦФ са регламентирани в политика за използване на крайни клиентски устройства.

4. Общи изисквания за използване на ИТ ресурсите

4.1 Всеки потребител се задължава:

1) Да защитава ИТ ресурсите в съответствие с изискванията, описани в Политика за информационна сигурност - Класификация на информацията;
2) Да предава/пренася информация от класификационно Ниво 1 само чрез одобрени от ИОХЦФ механизми;
3) Да съхранява информацията от класификационно Ниво 1 само на защитени носители;
4) Да работи само с информация, до която има разрешение за достъп или която е публична;
5) Да използва само легални версии на използваните програмни продукти, в съответствие с лицензионните изисквания на производителите;
6) Да използва собствените си устройства (Bring Your Own Device -BYOD), свързани към мрежите на OrgChmNet съгласно политиката за използване на крайни клиентски устройства;
7) Да съобщава за съмнително поведение на своите компютри, в резултат на всякакъв вид кибер атаки на звеното за ИТ услуги (IT.Services@orgchm.bas.bg);

4.2 На потребителите се забранява:

1) Да придобиват неправомерно достъп до други персонални системи, файлове и данни без да имат разрешение за това;
2) Да придобиват пароли или информация за други потребители, свързани с възможности за удостоверяване (придобиване на автентичност) и упълномощаване;
3) Да използват компютърни програми за декодиране на пароли или информация, свързана с възможности за удостоверяване и упълномощаване на други потребители;

4) Да създават или използват нелегални копия на патентовани програмни продукти, да съхраняват тези копия в системите на OrgChmNet или да ги предават чрез мрежите на OrgChmNet;
5) Да извършват действия, които могат да попречат на нормалната работа на OrgChmNet или да попречат на останалите потребители да използват ресурсите на OrgChmNet. Това включва подправяне на конфигурацията на компютрите, на периферните устройства, на мрежовите устройства, както и кабелната мрежа на ИОХЦФ;
6) Да заобикалят антивирусните системи, както и умишленото да въвеждат зловреден код като вируси, троянски кон, червеи, шпионски софтуер, рансъмуер[1] или подобни;
7) Нерегламентирано включване на устройства в розетките на локалната мрежа на ИОХЦФ. Необходимостта от включване на устройство в конкретна розетка от потребителя се подава писмено към звеното за ИТ услуги, като заявката се одобрява от ръководителя на лабораторията. Позволените устройства и процедурата по одобрение са описани в приложение;
8) Използването на служебната електронна поща, социалните мрежи и инструменти или други методи за съобщения в противоречие с нормативната уредба на страната или с цел злепоставяне на други хора. Например, разпространяването на информация чрез непрекъснато изпращане съобщения, които не са поискани е забранено;
9) Използването на системите и мрежите на OrgChmNet за търговски цели. Изключения – потребителите, които са наематели;

4.3 Всякакви опити от страна на потребителите за заобикаляне или разрушаване на ИТ системите за одит и сигурност са забранени и подлежат на санкции;

4.4. Позволява се включване на собствени устройства към безжичната (WiFi) мрежа на Института, като начинът на използване на безжичната мрежа е регламентиран в приложение;

4.5. Препоръчва се настройка на компютрите за режим Log Off или със заключен екран, в моментите, когато не работят;

4.8. Потребителите могат да използват софтуер на крайните устройства, в съответствие с политиката за използване на крайни клиентски устройства и програмното осигуряване на OrgChmNet.

5. Използване на ИТ потребителски сметки (акаунти)

5.1 Всеки потребител, в зависимост от своите права и задължения в ИОХЦФ, получава разрешение за използване на определени ИТ ресурси, което се управлява от системата за информационна сигурност.

5.2 Информационната сигурност за OrgChmNet се осигурява от система за контрол на достъпа, реализирана чрез услугите удостоверяване (автентикация) и упълномощаване на активната директория (Локална активна директория и Azure AD).

5.3 За всеки потребител, който достъпва и използва защитени ИТ ресурси се създава потребителски акаунт, включващ персонален идентификатор и парола. Всяко разрешение за използване на

[1] Рансъмуер е специфичен вид злонамерен софтуер, който изтръгва финансов откуп от жертвите си, като заплашва да публикува, изтрие или затвори достъпа до важни лични данни.

определени ресурси се управлява чрез задаване на права за достъп на акаунта до съответните услуги;

5.4. Потребителите отговарят индивидуално за използването на своите персонални пароли. Не се позволява предоставянето на индивидуалните пароли на други потребители;

5.5. Един потребител не може да използва персоналния акаунт на друг потребител;

5.6 Създаването и използването на акаунти и пароли се регламентира с политика за акаунтите и паролите.

6. Мониторинг и неприкосновеност на личността

6.1. ИТ координаторите на мрежата могат да извършват рутинни дейности, свързани с мониторинг на състоянието и използването на ИТ оборудването и ИТ услугите, с цел осигуряване непрекъсваемост на услугите, както и с цел откриване на зловреден код и/или опити от други видове кибер и фишинг атаки. В общия случай, това не включва наблюдение на индивидуалните комуникации или разкриване на съдържанието на потребителските файлове;

6.2. ИОХЦФ си запазва правото да извършва мониторинг на индивидуалното използване на ИТ оборудването и ИТ услугите от даден потребител, включващо електронната поща (изпращани и получавани писма), Web страници и друго онлайн съдържание, до които потребителят е имал достъп, с цел:

6.2.1. Защита на ИТ инфраструктурата от вируси, хакерски, фишинг или други кибер атаки;

6.2.2. Подпомагане на анализа при възникнали хакерски, фишинг или други кибер атаки;

6.2.3. Предотвратяване или откриване на престъпно или друго нерегламентирано използване на ИТ ресурсите на института;

6.2.4. При изискване по закон, например от държавните или други упълномощени власти;

6.2.5. Мониторингът на индивидуалното използване на ИТ ресурсите на ИОХЦФ се извършва при всички случаи след разрешение от директора на института, като задължително се извършва предварителен анализ на въздействието от това действие. Наблюдението се извършва за максимален период, не по-дълъг от три месеца, и може да бъде продължено след актуализиране на оценката на въздействието.

6.3. Цялата информация, събрана по времето на всяко наблюдение се съхранява по сигурен начин, в съответствие с изискванията на политиката за информационна сигурност;

6.4. Потребител, който е бил обект на мониторинг има право да се запознае със събраните данни и причините за дисциплинарните или други последствия, които могат да настъпят.

7. ИТ услуги на OrgChmNet

7.1 OrgChmNet предоставя на потребителите набор от ИТ услуги, описани в Каталог на услугите. ИТ услугите на OrgChmNet са предназначени основно за осигуряване на академичната и оперативната дейност на ИОХЦФ, за подпомагане на научния персонал, научно-помощния персонал, администрацията и обучаващите се. Определени ИТ услуги се предоставят на партньори и гости на института, както и на наемателите в сградата на ИОХЦФ.

7.2 Правилата за използването на някои специфични ИТ услуги на OrgChmNet се регламентират допълнително чрез приложения към настоящата политика. За всяка такава ИТ услуга, която е влязла в експлоатация се създава и публикува отделно Приложение. Настоящият документ, заедно с всички негови приложения регламентират Политиката за използване на ИТ ресурсите.

7.3 ИТ услугите се изграждат и поддържат от звеното **ИТ услуги** (IT.Services@orgchm.bas.bg)

7.4 Звеното ИТ услуги не поддържа крайни клиентски устройства, които не са част от вътрешната мрежа (домейна) на ИОХЦФ.

8. Информираност и санкции

8.1. Тази политика се предоставя на всички съществуващи, асоциирани и нови служители на ИОХЦФ, обучаващите се в института, наематели и гости на ИОХЦФ. Препоръчва се на всички останали потребители на информационните ресурси на ИОХЦФ да се информират за съществуването на тази политика от интернет страницата на ИОХЦФ (https://www.orgchm.bas.bg/vutreshna.html);

8.2. Всички потребители са длъжни да се запознаят подробно с тази политика и да спазват нейните изисквания;

8.3. При възникване на предполагаемо нарушение на изискванията, ще бъдат предприети всички разумни действия, за да се провери твърдението за нарушение. Ако твърдението за нарушение се потвърди, ще бъдат предприети необходимите стъпки за предотвратяване на по-нататъшни злоупотреби. Това може да включва упълномощена проверка на файловете на потребителя или неговата електронна поща, съгласно т. 6.2 от настоящата политика;

8.4. При подадена жалба или нарушение на потребител на ИТ ресурсите на ИОХЦФ, достъпът му може да бъде спрян незабавно, без предизвестие. Когато е възможно, потребителите ще бъдат уведомявани за такова спиране на достъпа;

8.5. Санкциите за нарушаване на тази политика могат да доведат до начало на дисциплинарни процедури, включително и уволнение. При определени обстоятелства могат да бъдат предприети и правни действия;

8.6. При установяване на нерегламентиран достъп до информация, съдържаща лични данни, следва незабавно да се докладва на длъжностното лице по защита на личните данни в канцеларията на ИОХЦФ в съответствие с изискванията на Закона за защита на личните данни;

8.7. При проверка в ИОХЦФ установяваща, че може да е извършено престъпление, може да бъдат уведомени и българските право охранителни органи, които ще получат и съдействие от Института в хода на техните разследвания;

8.8. Всяко физическо проникване, свързано с ИТ оборудването, следва да се докладва на звеното за ИТ услуги (IT.Services@orgchm.bas.bg);

Vanya Bogdanova Kurteva-Lukanova

Digitally signed by Vanya Bogdanova Kurteva-Lukanova
Date: 2022.01.17 15:47:00 +02'00'