32.СРЕДНО УЧИЛИЩЕ С ИЗУЧАВАНЕ НА ЧУЖДИ ЕЗИЦИ
„СВЕТИ КЛИМЕНТ ОХРИДСКИ“

гр. София, бул. „Христо Ботев“ №63, тел.: 02/9874358,
email: kl_ohridski32@school32.com

УТВЪРЖДАВАМ:

Д-Р НЕЛИ КИРКОВА-КОСТОВА,

ДИРЕКТОР НА 32. СУИЧЕ

ПОЛИТИКА ЗА МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ В 32. СРЕДНО УЧИЛИЩЕ С ИЗУЧАВАНЕ НА ЧУЖДИ ЕЗИЦИ „СВЕТИ КЛИМЕНТ ОХРИДСКИ“

РАЗДЕЛ I.
ОБЩИ ПОЛОЖЕНИЯ

Политика за мрежова и информационна сигурност в 32. СУИЧЕ е изготвена в съответствие с изискванията на Закона за електронното управление, Закона за киберсигурност и Наредбата за минималните изисквания за мрежова и информационна сигурност.

Чл. 1. Основната цел на Политиката за мрежова и информационна сигурност е да определи необходимите мерки и дейности за постигане на високо общо ниво на мрежова и информационна сигурност в 32.СУИЧЕ.

Чл. 2. Настоящата политика за мрежова и информационна сигурност определя ред, отговорности, способи и средства при осъществяване контрол и управление на работата на информационните системи в 32. СУИЧЕ.

Чл. 3. Информационната система се определя като съвкупност от компютърна и периферна техника, програмни продукти, данни и обслужващ персонал, като компютрите могат да бъдат свързани в локална мрежа или по друг начин, както и да обменят информация чрез съответните устройства и програми.

Чл. 4. Политиката за мрежова и информационна сигурност е набор от документи, правила и норми за поведение, които определят как 32. СУИЧЕ защитава обработката, съхранението и разпространението на информацията.

Чл. 5. Политиката за мрежова и информационна сигурност касае работата на всички служители в училището, които са длъжни със своите действия да гарантират ефективното и ефикасно използване на системите.

Чл. 6. Политиката има включва всички съответни специфични политики за сигурност на информационните и комуникационните системи, като обмен на информация,
използване на мобилни устройства, работа от разстояние, управление на достъпите и автентикацията, управление на инциденти, взаимоотношение с трети страни, повишаване на квалификацията на служителите и на осведомеността по отношение на мрежовата и информационната сигурност.

Чл. 7. Мрежова и информационна сигурност е способността на мрежите и информационните системи да се противопоставят на определено ниво на въздействия, засягащи отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или на свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях.
Чл. 8. (1) Мерките за мрежова и информационна сигурност са организационни, технологични и технически и се прилагат в съответствие със спецификата на дейността на 32.СУИЧЕ и пропорционално на заплахите с цел минимизиране на риска от тяхното реализиране.
(2) Мерките по ал.1 гарантират основните цели на мрежовата и информационната сигурност, а именно запазване на достъпността, интегритета (цялост и наличност) и конфиденциалността на информацията по време на целия ѝ жизнен цикъл (създаване, обработване, съхранение, пренасяне и унищожение) във и чрез информационните и комуникационните системи на 32.СУИЧЕ.
(3) Минималните организационни мерки, които се прилагат са:
1. разпределение на отговорностите за мрежовата и информационната сигурност;
2. прилагане на политика за мрежовата и информационната сигурност;
3. управление на:
а) риска;
б) информационните активи, включително човешките ресурси;
в) инцидентите;
г) достъпите (физически и логически);
д) измененията;
е) непрекъснатостта на дейността и/или услугите (съществени, цифрови);
ж) взаимодействията с трети страни.
Чл. 9. Проектирането и изграждането на информационни и комуникационни системи в 32.СУИЧЕ се извършва така, че те да представляват компоненти с възможност за интеграция в единна потребителска среда и при спазване на Наредбата за общите изисквания за оперативна съвместимост и информационна сигурност.

РАЗДЕЛ II.
УПРАВЛЕНИЕ НА МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ КОНТРОЛ НА ДОСТЪПА И ПРАВИЛА ЗА РАБОТА С НОСИТЕЛИ

Разпределение на роли и отговорности
Чл. 10. (1) Директорът на 32.СУИЧЕ:
1. носи пряка отговорност за мрежовата и информационната сигурност, дори и когато дейността е възложена за изпълнение на трети страни;
2. създава условия за прилагане на комплексна система от мерки за управление на тази сигурност; системата обхваща всички области на сигурност, които засягат мрежовата и информационната сигурност на училището, включително физическата сигурност на информационните и комуникационните системи;
3. осигурява необходимите ресурси за прилагане на пропорционални и адекватни на рисковете организационни, технически и технологични мерки, гарантиращи високо ниво на мрежова и информационна сигурност, съгласно нормативната база;
4. упражнява контрол върху нивото на мрежовата и информационната сигурност чрез провеждане минимум веднъж в годината на периодичен преглед на мрежовата и информационната сигурност и на адекватността на предприетите мерки;
5. определя, документира и налага отговорности по изпълнението, контрола и информираността за всички процеси и дейности, свързани с развитието, поддръжката и експлоатацията на информационните и комуникационните системи, като се спазва принципът, че едно лице не може да контролира собствената си дейност.
(2) Директорът на 32.СУИЧЕ определя служител, отговарящ за мрежовата и информационната сигурност, като:

1. Служителят, отговарящ за мрежовата и информационната сигурност, е на пряко подчинение на директора на училището, с цел пряко информиране за състоянието и проблемите в мрежовата и информационната сигурност;
2. Препоръчителните функции на служителя, отговарящ за мрежовата и информационната сигурност, са следните:
2.1. Ръководи дейностите, свързани с постигане на високо ниво на мрежова и информационна сигурност;
2.2. Участва в изготвянето на политиките и документираната информация.
2.3. Следи за спазването на вътрешните правила за мрежовата и информационната сигурност;
2.4. Консултира ръководството на училището във връзка с информационната сигурност;
2.5. Координира обученията, свързани с мрежовата и информационната сигурност;
2.6. Поддържа връзки с други администрации, организации и експерти, работещи в областта на информационната сигурност;
2.7. Уведомява за инциденти с компютърната сигурност;
2.8. Следи за актуализиране на използвания софтуер и фърмуер;
2.9. Следи за появата на нови киберзаплахи (вируси, зловреден код, спам, атаки и др.) и предлага адекватни мерки за противодействието им.
3. Служителят, отговарящ за мрежовата и информационната сигурност осъществява функциите съвместно с представител/и на фирмата/фирмите, с която/които 32.СУИЧЕ има сключен договор за поддръжка на използвания в училището хардуер.
Чл. 11. (1) За намаляване на загубите от инциденти чрез намаляване на времето за реагиране и разрешаването им, както и за намаляване на вероятността от възникване на инциденти, породени от човешки грешки, в училището се разработват:
1. Вътрешни правила за служителите, указващи правата и задълженията им като потребители на услугите, предоставяни чрез информационните и комуникационните системи, като използване на персонални компютри, достъп до ресурсите на училищната мрежа, генериране и съхранение на паролите, достъп до интернет, работа с електронна поща, електронни платформи, системи за документооборот и други вътрешноведомствени системи, принтиране, използване на сменяеми носители на информация в електронен вид, използване на преносими записващи устройства и т. н.
2. Правила за работа в компютърен кабинет, касаещи правата и задълженията на учениците.
(2) Вътрешните нормативни документи, касаещи мрежовата и информационна сигурност в 32.СУИЧЕ се преглеждат и актуализират поне веднъж годишно и/или при необходимост.
(3) Вътрешните нормативни документи се утвърждават от директора на училището и се свеждат до знанието на всички служители и ученици срещу подпис.
Чл. 12. Защитата и контролът на информационните и компютърните системи се извършва при спазване на следните основни принципи:
- разделяне на потребителски от администраторски функции;
- установяване на нива и достъп до информация;
- регистриране на достъпа, въвеждането, промяната и заличаването на данни и информация;
- осъществяването на контрол.

Чл. 13. Всеки служител има точно определени права на достъп и използва уникален потребителски профил за вход в системата и достъп до данните, за които е оторизиран, така че да може да бъде идентифициран. Не е разрешено използването на групови профили.
Чл. 14. Контрол на управлението и защитата на достъпа до мрежови връзки и мрежови услуги се извършва от Системния администратор/и, който контролира компютрите, използвани за достъп до мрежи и мрежови услуги.

Чл. 15. Предоставянето на достъп става по дефиниран вътрешен ред, като се задават определени права на достъп до конкретни информационни ресурси, според заемната длъжност и функция. Не се задава и не се осигурява достъп на неоторизирани лица.
Чл. 16. Лицата, които обработват лични данни, използват достатъчно сложни и уникални пароли, които не се записват или съхраняват онлайн. Индивидуалните пароли не се използват съвместно с други потребители.
Чл. 17. Всички пароли за достъп на системно ниво се променят периодично.
Чл. 18. Всички носители на лични данни се съхраняват в безопасна и сигурна среда - в съответствие със спецификациите на производителите, в заключени шкафове, с ограничен и контролиран достъп.

Управление на риска

Чл. 19. (1) В 32.СУИЧЕ е разработен утвърден документ „Стратегия за управление на риска“. Оценката на мрежовата и информационната сигурност се извършва регулярно, но не по-рядко от веднъж годишно, или когато се налагат съществени изменения в целите, вътрешните и външните условия на работа, информационната и комуникационната инфраструктура, дейностите или процесите.
(2) На основание на анализа и оценката на риска се изготвя план за намаляване на неприемливите рискове, който да включва минимум:
1. подходящи и пропорционални мерки за смекчаване на неприемливите рискове;
2. необходими ресурси за изпълнение на тези мерки;
3. срок за прилагане на мерките;
4. отговорни лица.

Защита

Чл. 20. (1) 32.СУИЧЕ прилага следните мерки за защита на профилите с административни права за информационните и комуникационните системи и техните компоненти:
1. преди въвеждане в експлоатация задължително се сменят идентификационните данни на администратора, въведени по подразбиране или инсталирани от производителя/доставчика на
информационния актив;
2. администраторските профили са персонални;
3. администраторските профили се използват само за административни цели;
4. администраторските профили се създават само на служители, които извършват административни операции (инсталиране, конфигуриране, управление, поддръжка и т. н.);
5. правата на всеки администраторски акаунт са ограничени във възможно най-голяма степен до функционалния и техническия периметър на всеки администратор;
6. данните за автентикацията на администраторските акаунти:
а) са различни за всяка система;
б) са с възможно най-голяма сложност, позволена от системата или нейния компонент;
в) се съхраняват подходящо физически и логически защитени, като достъп до тях има само оторизиран представител на Субекта;
7. поддържа списък на администраторските профили за информационните и комуникационните системи и техните компоненти;
8. при невъзможност на администратор да изпълнява пълноценно функциите си поради обективни причини правата на административния му акаунт се спират за съответния период;
9. поне веднъж годишно се прави преглед на администраторските профили с цел удостоверяване на актуалността им.
(2) Паролите за автентикация на администраторските профили се сменят задължително:
1. периодично - най-малко веднъж в годината;
2. при прекратяването на договорните отношения със служители или трети страни, на които тези данни са били известни;
3. при пробив в мрежовата и информационната сигурност.

Чл. 21. (1) В 32.СУИЧЕ се инсталират и поддържат само версии на използвания в системите му софтуер, които се поддържат от техните доставчици или производители и са актуални от гледна точка на сигурността.
(2) В 32.СУИЧЕ са предприети мерки за:
1. недопускане на инсталирането и използването на неодобрен софтуер и фърмуер;
2. контрол върху използвания софтуер и фърмуер, включително неговата актуалност.
Чл. 22. (1) Училището прилага подходящи мерки за защита от проникване и мерки за откриване и справяне със зловреден софтуер.
(2) Мерките за защита от зловреден софтуер трябва:
1. да са приложени към всички компоненти на информационните и комуникационните системи, където това е възможно;
2. да се поддържат в актуално състояние, за да имат способността да защитават от новооткрити заплахи.
(3) Мерките за защита от зловреден софтуер трябва да позволяват:
1. извършване на пълна проверка за наличие на зловреден софтуер поне веднъж в седмицата, където е приложимо;
2. проверка на електронната поща и файлове, свалени от интернет, както и преносими записващи устройства, преди да бъдат отворени.
(4) В училището регулярно се извършва оценка на ефективността на мерките за защита от зловреден софтуер и при констатирани слабости предприема действия за подобряване на защитата.
Защита на уеб сървъри
Защита на Domain Name System (DNS)
Чл. 23. (1) Субектът предприема следните мерки за защита:
В училището работи domain controller
Домейн контролерите са разположени върху два Hyper-V хоста/сървъра и работят като виртуални машини, като единия домейн контролер (виртуалната машина) се репликира върху другия Hyper-V хост. В хардуерният firewall са зададени политики за трафика със съответните ограничения. На всички компютри има инсталиран ESET NOD32 Antivirus, и се използват Windows Defender и Microsoft Security.

РАЗДЕЛ III.
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Всички служители в 32.СУИЧЕ са длъжни да познават и спазват разпоредбите на тази Политика.
§ 2. Контролът по спазване на Политиката се осъществява от Директора на училището или упълномощено със заповед лице (системен администратор).
§ 3. Настоящата Политика се разглежда и оценява периодично с оглед ефективността й, като ръководството на 32.СУИЧЕ може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.
§ 4. Настоящата политика подлежи на актуализация при промяна на нормативната база.
§ 5. Политиката е утвърдена със заповед на директора на 32. СУИЧЕ „Св. Климент Охридски“ № ……../……...г. и влиза в сила от датата на утвърждаването й.