



REGULI DE IGIENĂ CIBERNETICĂ

Igiena cibernetică înseamnă măsuri preventive și comportamente zilnice care protejează confidențialitatea, integritatea și disponibilitatea informațiilor. Este necesară din cauza amenințărilor și ca obligație legală/profesională a membrilor organelor electorale, funcționarilor aparatelor de lucru, registratorilor pentru protecția datelor și continuitatea serviciilor.



Regula 1: Parola e personală, confidențială și netransmisibilă!

- Păstrați plicul cu parola într-un loc sigur.
- NU fotografiați, NU copiați și NU partajați parola cu nimeni, indiferent de funcție!
- Apelați la Comisia Electorală Centrală pentru a schimba parola imediat dacă bănuți că a fost compromisă.



Regula 2: Evitați aglomerarea mesei de lucru!

- Birou curat: strângeți documentele sensibile și nu lăsați notițe adezive cu parole pe birou.
- Ecran curat: blocați ecranul calculatorului când plecați (apăsând concomitent Win+L).



Regula 3: USB – Virus potențial

- Este interzisă conectarea dispozitivelor USB de stocare neautorizate.
- Folosiți doar dispozitive aprobate și scanați-le înainte de a le utiliza.
- Evitați de a primi stick-uri USB cadou la conferințe sau evenimente.



Regula 4: Fiți atenți ce postați pe rețelele sociale!

- Nu publicați date de serviciu, fotografii din birou cu documente pe fundal sau planuri interne.
- Verificați setările de confidențialitate la fiecare actualizare.



Regula 5: NU înghiți momeala!

- Phishing-ul (mesaj fals trimis pentru a fura date personale sau parole) apare prin e-mail, SMS sau chat-uri „urgente”.
- Verificați expeditorul, linkurile și fișierele atașate. Când aveți dubii, nu deschideți nimic!
- Nu oferiți informații despre conturi, sisteme sau parole nimănui, indiferent de funcția declarată.



Regula 6: Actualizați și reporniți!

- Instalați actualizările de sistem Windows și ale aplicațiilor pentru a beneficia de cele mai recente pachete de securitate.
- Reporniți periodic calculatorul pentru ca actualizările să se instaleze corect.



Regula 7: Separați munca de viața personală

- Nu folosiți e-mailul personal pentru documente de serviciu și invers.
- Nu instalați aplicații neaprobată pe calculatorul sau laptopul instituției.



Regula 8: Raportați incidentele!

- Dacă ați observat ceva ciudat pe calculatorul/laptopul instituției sau în rețea anunțați imediat responsabili de la CEC: *Direcția tehnologii informaționale și gestionarea listelor electorale (DTIGLE) din cadrul Aparatului Comisiei Electorale Centrale:*

☎ 022-88-01-01 ☎ it@cec.md

Rapiditatea salvează datele!





CICDE

Centrul de Instruire Continuă
în Domeniul Electoral

ПРАВИЛА КИБЕРГИГИЕНЫ

Кибергигиена — это совокупность профилактических мер и ежедневных привычек, которые защищают конфиденциальность, целостность и доступность информации. Она необходима из-за киберугроз и является правовой и профессиональной обязанностью членов избирательных органов, сотрудников секретариата и регистраторов для защиты данных и обеспечения непрерывности публичных услуг.



Правило 1: Пароль как зубная щётка: личный и не передаётся никому!

- Храните конверт с паролем в надёжном месте.
- Не фотографируйте, не копируйте и не передавайте пароль никому, независимо от должности!
- Обратитесь в Центральную избирательную комиссию для немедленной смены пароля, если подозреваете, что он был скомпрометирован.



Правило 2: Порядок на рабочем месте!

- Чистый стол: убирайте конфиденциальные документы, не оставляйте стикеры с паролями на столе.
- Чистый экран: блокируйте экран компьютера, когда выходите из кабинета (нажмите одновременно клавиатурные клавиши «Win+L»).



Правило 3: USB-носители — потенциальный источник вирусов!

- Подключение неавторизованных USB-накопителей запрещено.
- Используйте только одобренные устройства и сканируйте их антивирусом перед использованием.
- Старайтесь не принимать USB-накопители в качестве подарков на конференциях или мероприятиях.



Правило 4: Внимательно относитесь к публикациям в социальных сетях!

- Не публикуйте служебные данные, фотографии из офиса с документами на заднем фоне или внутренние планы.
- Проверяйте настройки конфиденциальности при каждом обновлении.



Правило 5: Не клуйте на приманку!

Фишинг — это поддельные сообщения по электронной почте, SMS или в «срочных» чатах для кражи персональных данных или паролей.

- Проверяйте отправителя, ссылки и вложения. Если сомневаетесь — ничего не открывайте!
- Не сообщайте никому данные учётных записей, сведения о системах или пароли — независимо от заявленной должности.



Правило 6: Обновляйте и перезагружайте систему!

- Устанавливайте обновления Windows и приложений, чтобы получать актуальные пакеты безопасности.
- Регулярно перезагружайте компьютер для корректного применения обновлений системы и программ



Правило 7: Отделяйте работу от личной жизни!

- Не используйте личную почту для служебных документов и наоборот.
- Не устанавливайте на служебный компьютер/ноутбук неподтверждённые приложения.



Правило 8: Сообщайте об инцидентах!

- Если заметили что-то необычное на служебном компьютере/ноутбуке или в сети, немедленно сообщите об этом ответственным сотрудникам ЦИК:
Управление информационных технологий и по ведению списков избирателей (DTIGLE) из состава Аппарата Центральной избирательной комиссии:

☎ 022-88-01-01 📧 it@cec.md

Оперативность спасает данные!



**UK International
Development**

Partnership | Progress | Prosperity



Этот материал подготовлен при содействии проекта Международного Фонда Избирательных Систем (IFES) «Поддержка выборов в Молдове», финансируемого Департаментом международного развития правительства Соединенного Королевства, но выраженные в нем мнения не обязательно отражают официальную политику британского правительства.