Advocacy Center
for Democratic Culture

PRAKTIKAT E SIGURISË KIBERNETIKE NË INTERNET DHE PROCEDURAT E SIGURISË DIGJITALE

Miratuar: 2026

Vlen për: të gjithë punonjësit, konsulentët, vullnetarët dhe bashkëpunëtorët e jashtëm

www.acdc-kosovo.org

1. Qëllimi dhe Fushëveprimi

Ky dokument përcakton standardet e brendshme të sigurisë kibernetike, rregullat e sigurisë digjitale dhe mekanizmat e mbrojtjes së të dhënave të ACDC. Qëllimi kryesor i tij është të sigurojë mbrojtjen e të dhënave të ndjeshme të organizatës, informacionit të donatorëve, të dhënave të përfituesve, dokumentacionit financiar dhe sistemeve të komunikimit.
Kjo politikë përcakton masa parandaluese kundër kërcënimeve kibernetike si phishing, përpjekje për hakerim, infeksione me malware, inxhinieri sociale, vjedhje identiteti dhe qasje të paautorizuar në platformat digjitale.
Këto procedura zbatohen për të gjitha zyrat e ACDC-së (Mitrovica e Veriut, Prishtina, Beogradi), duke përfshirë të gjitha pajisjet zyrtare, serverët, shërbimet cloud, faqet e internetit, platformat e mediave sociale, bazat e brendshme të të dhënave dhe mjetet e komunikimit që përdoren për qëllime profesionale.

2. Rreziqet e Identifikuara dhe Reagimi Organizativ

Pas vlerësimeve të brendshme dhe incidenteve të mëparshme kibernetike, përfshirë shkeljen e llogarive zyrtare në rrjetet sociale, ACDC identifikoi disa dobësi strukturore dhe operacionale. Këto përfshinin rutim të paqëndrueshëm të internetit, mungesë të ruajtjes së centralizuar të të dhënave, përdorim të pamjaftueshëm të autentifikimit me shumë faktorë dhe ndërgjegjësim të kufizuar të stafit për sigurinë kibernetike.

Si përgjigje ndaj kësaj, ACDC zbatoi masa gjithëpërfshirëse korrigjuese, duke përfshirë:

- Adoptimin e Starlink si ofrues zyrtar të internetit për të siguruar lidhje të qëndrueshme dhe të sigurt.
- Krijimin e profileve zyrtare Meta Business me qasje të kontrolluar administrative.
- Instalimin e një serveri të brendshëm të centralizuar për menaxhimin e sigurt të dokumenteve.
- Implementimin e softuerit antivirus në të gjitha pajisjet zyrtare.
- Trajnime të detyrueshme për stafin mbi sigurinë kibernetike.
- Vendosjen e protokolleve të brendshme për reagim ndaj incidenteve.

Këto masa reduktojnë ndjeshëm rreziqet operacionale dhe forcojnë reziliencën digjitale të organizatës.

3. Siguria e Internetit dhe Rrjetit

ACDC përdor Starlink si ofrues zyrtar të shërbimit të internetit për të siguruar qasje të qëndrueshme, të enkriptuar dhe të besueshme në internet. Infrastruktura e rrjetit është e mbrojtur me fjalëkalim dhe kredencialet e qasjes janë të kufizuara vetëm për personelin teknik të autorizuar.

- Organizata zbaton standardet e mëposhtme të sigurisë së rrjetit:
- Enkriptim të fortë të fjalëkalimeve në nivel ruteri.
- Ndryshime periodike të fjalëkalimeve.
- Ndarje të rrjetit të brendshëm dhe qasjes për mysafirë (kur është e aplikueshme).
- Kufizime për qasje të largët.
- Monitorim të aktivitetit të pazakontë të rrjetit.

Instalimi i paautorizuar i pajisjeve të rrjetit ose ndarja e kredencialeve të rrjetit është rreptësisht e ndaluar.

4. Serveri i Centralizuar dhe Menaxhimi i të Dhënave

ACDC ka implementuar një server të brendshëm të centralizuar për të rregulluar ruajtjen e skedarëve, për të reduktuar varësinë nga transferimet e jashtme të dokumenteve dhe për të siguruar menaxhim të strukturuar të dokumenteve.
Serveri ofron:

- Qasje të kontrolluar bazuar në rolet e stafit.
- Ruajtje të sigurt të dokumentacionit financiar, ligjor dhe programor.
- Reduktim të varësisë nga pajisjet personale për ndarjen e dokumenteve.
- Arkitekturë të organizuar të të dhënave për të parandaluar dublimin dhe humbjen e të dhënave.

Kopjet rezervë krijohen rregullisht dhe ruhen në mjedise të mbrojtura. Shërbimet cloud të përdorura nga ACDC mbrohen me autentifikim me dy faktorë dhe procedura kontrolli të qasjes. Të drejtat e qasjes revokohen menjëherë pas përfundimit të marrëdhënies së punës ose bashkëpunimit me konsulentë.

5. Siguria e Pajisjeve

Të gjithë laptopët dhe kompjuterët zyrtarë janë të pajisur me softuer antivirus të licencuar (p.sh. **NOD32** ose ekuivalent). Përditësimet automatike të sigurisë janë të aktivizuara për të siguruar mbrojtje nga kërcënimet e reja.
Standardet e përdorimit të pajisjeve përfshijnë:

- Mbrojtje të detyrueshme me fjalëkalim për të gjitha pajisjet.
- Bllokim automatik të ekranit pas periudhave të pasivitetit.
- Ndalim të instalimit të softuerëve të paautorizuar.
- Ndalim të përdorimit të kompjuterëve publikë për qasje në llogari zyrtare.
- Ruajtje të sigurt të pajisjeve kur nuk janë në përdorim.

Pajisjet USB dhe disqet e jashtme duhet të skanohen para përdorimit. Pajisjet e humbura ose të vjedhura duhet të raportohen menjëherë.

6. Mbrojtja e Mediave Sociale dhe Prania Online

Pas qasjes së paautorizuar në llogaritë e mediave sociale, ACDC ka forcuar menaxhimin e platformave digjitale.

Masat përfshijnë:

- Përdorimin vetëm të llogarive zyrtare Meta Business Suite.
- Autentifikim të detyrueshëm me dy faktorë në të gjitha platformat e mediave sociale.
- Qasje administrative të bazuar në role (Primar: Zyrtari i Komunikimit; Rezervë: Drejtori Ekzekutiv).
- Heqje të menjëhershme të qasjes për ish-punonjësit.
- Ruajtje të sigurt të fjalëkalimeve përmes mjeteve për menaxhimin e fjalëkalimeve.

Vetëm stafi i autorizuar ka të drejtë të publikojë ose menaxhojë përmbajtje zyrtare.

.

7. Siguria e Email-it dhe Komunikimit

Të gjitha komunikimet zyrtare duhet të realizohen përmes llogarive email me domenin @acdc-kosovo.org.
Stafi trajnohet për të identifikuar email-e phishing, bashkëngjitje të dyshimta dhe lidhje të rrezikshme.
Procedurat e sigurisë përfshijnë:

- Ndalimin e shkarkimit të bashkëngjitjeve të panjohura.
- Verifikimin e email-eve të dyshimta me dërguesin përmes një kanali tjetër komunikimi.
- Raportimin e menjëhershëm të tentativave të phishing.
- Përditësimin e rregullt të fjalëkalimeve dhe aktivizimin e autentifikimit me dy faktorë.

Të dhënat konfidenciale të donatorëve dhe përfituesve nuk duhet të ndahen përmes aplikacioneve të pasigurta të komunikimit.

8. Zhvillimi i Kapaciteteve të Stafit dhe Ndërgjegjësimi

Duke e njohur faktin se gabimi njerëzor është një nga dobësitë kryesore në sigurinë kibernetike, ACDC organizon trajnime të strukturuara për të rritur ndërgjegjësimin e stafit për rreziqet digjitale.
Temat e trajnimeve përfshijnë:

- Identifikimin e tentativave të phishing dhe faqeve të dëmshme.
- Praktika të sigurta të shfletimit dhe menaxhimit të fjalëkalimeve.
- Trajtimin e sigurt të të dhënave të ndjeshme.
- Higjienën digjitale dhe standardet e privatësisë.
- Përdorimin e përgjegjshëm dhe etik të mjeteve të inteligjencës artificiale.

Trajnimi për sigurinë kibernetike është pjesë e procedurave të orientimit për punonjësit dhe vullnetarët e rinj.

9. Politika e Fjalëkalimeve

ACDC zbaton standarde të forta për fjalëkalimet:

- Minimumi 12 karaktere.
- Kombinim i shkronjave të mëdha dhe të vogla, numrave dhe simboleve.
- Mosripërdorimi i të njëjtit fjalëkalim në platforma të ndryshme.
- Rekomandohet përdorimi i menaxherëve të fjalëkalimeve.
- Fjalëkalimet nuk duhet të ndahen përmes email-it ose aplikacioneve të komunikimit.

Ndryshimi periodik i fjalëkalimeve është i detyrueshëm për llogaritë administrative me nivel të lartë qasjeje.

10. Procedura e Reagimit ndaj Incidenteve

Në rast të dyshimit për incident të sigurisë kibernetike, duhet të ndërmerren menjëherë këto hapa:

1. Shkëputni pajisjen e prekur nga interneti.
2. Njoftoni Drejtorin Ekzekutiv dhe Zyrtarin e Komunikimit.
3. Ndryshoni fjalëkalimet e kompromet uara.
4. Dokumentoni detajet e incidentit.
5. Informoni partnerët ose donatorët përkatës nëse është e nevojshme.
6. Riktheni sistemet nga kopjet rezervë të sigurta nëse kërkohet.

Pas incidentit realizohet një analizë për të identifikuar shkaqet dhe për të parandaluar përsëritjen.

11. Mbrojtja e të Dhënave dhe Konfidencialiteti

ACDC trajton të dhënat personale, financiare dhe ligjore të ndjeshme me konfidencialitet të rreptë.

Masat përfshijnë:

- Qasje të kufizuar në të dhënat personale të përfituesve.
- Ruajtje të sigurt të dokumentacionit ligjor.
- Detyrime për moszbulim për stafin dhe konsulentët.
- Shpërndarje të kontrolluar të informacionit financiar.
- Përputhje me parimet e mbrojtjes së të dhënave.

Informacioni i ndjeshëm nuk duhet të ruhet në pajisje personale pa autorizim.

12. Monitorimi dhe Rishikimi

Kjo politikë e sigurisë kibernetike rishikohet çdo vit dhe përditësohet në përputhje me zhvillimet teknologjike dhe rritjen e organizatës. Përmirësimet në sigurinë kibernetike do të integrohen në kornizën strategjike të ACDC për periudhën 2026–2030, duke siguruar reziliencë digjitale afatgjatë dhe gatishmëri për situata krize.

13. Pajtueshmëria

Të gjithë punonjësit, konsulentët dhe vullnetarët janë të detyruar të respektojnë këtë politikë. Mosrespektimi i standardeve të sigurisë kibernetike mund të rezultojë në masa disiplinore të brendshme. Drejtori Ekzekutiv dhe menaxhmenti i programeve mbikëqyrin zbatimin dhe respektimin e kësaj politike.

www.acdc-kosovo.org

office@acdc-kosovo.org

www.facebook.com/Ngoacdc

www.instagram.com/acdc.kosovo

www.x.com/ngo_acdc