					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P20					Τίτλος εγγράφου: **Πολιτική Προστασίας Τερματικών Σημείων από Κακόβουλο Λογισμικό**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	Ρήτρα/Άρθρο	Σχόλιο
ISO/IEC 27001:2022	Ρήτρα 8	Απαιτούνται έλεγχοι για την προστασία τερματικών σημείων και την άμυνα κατά του κακόβουλου λογισμικού, ώστε να επιτυγχάνονται οι στόχοι του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS)
ISO/IEC 27002:2022	Έλεγχοι 8.7, 8	Παρέχει τεχνικούς ελέγχους και κατευθύνσεις για την άμυνα κατά του κακόβουλου λογισμικού, την προστασία τερματικών σημείων και τη διαχείριση περιστατικών
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Ορίζει απαιτήσεις για προστασία από κακόβουλο κώδικα, κεντρική παρακολούθηση και βασικές γραμμές ρυθμίσεων
ΓΚΠΔ της ΕΕ	Άρθρο 32	Επιβάλλει κατάλληλα τεχνικά μέτρα για τη διασφάλιση των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από κακόβουλο λογισμικό
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(d)	Απαιτεί την εφαρμογή μέτρων ανίχνευσης απειλών και πρόληψης σε επίπεδο τερματικού σημείου
Κανονισμός DORA της ΕΕ	Άρθρο 9	Απαιτεί αρμοδιότητες διαχείρισης κινδύνων ΤΠΕ για την άμυνα έναντι κακόβουλου λογισμικού και απειλών που προέρχονται από τερματικά σημεία
COBIT 2019	DSS05.01, DSS01.04, MEA	Απαιτεί προστασία, παρακολούθηση και αξιολόγηση των ελέγχων ασφάλειας στα τερματικά σημεία

1. Σκοπός

1.1 Η παρούσα πολιτική ορίζει τους υποχρεωτικούς ελέγχους και τις επιχειρησιακές απαιτήσεις για την προστασία των τερματικών σημείων του οργανισμού — συμπεριλαμβανομένων επιτραπέζιων υπολογιστών, φορητών υπολογιστών, φορητών συσκευών και διακομιστών — από κακόβουλο λογισμικό και συναφείς απειλές.

1.2 Καθορίζει τα ελάχιστα πρότυπα για την προστασία τερματικών σημείων, την ανίχνευση κακόβουλου λογισμικού, τις ενέργειες περιορισμού και την παρακολούθηση συμπεριφοράς, διασφαλίζοντας ότι τα συστήματα παραμένουν ανθεκτικά έναντι τόσο κοινών όσο και προηγμένων παραλλαγών κακόβουλου λογισμικού.

1.3 Η πολιτική υποστηρίζει άμεσα τη συμμόρφωση με το ISO/IEC 27001:2022, Ρήτρα 8.1, και το Παράρτημα Α, Έλεγχος 8.7, και είναι ευθυγραμμισμένη με περιφερειακές υποχρεώσεις κυβερνοασφάλειας βάσει του ΓΚΠΔ της ΕΕ, της Οδηγίας NIS2 της ΕΕ και του Κανονισμού DORA της ΕΕ.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε όλα τα τερματικά σημεία, συμπεριλαμβανομένων των εξής:

2.1.1 Επιτραπέζιοι υπολογιστές, φορητοί υπολογιστές, φορητές συσκευές και εικονικές παρουσίες που ανήκουν στον οργανισμό ή τελούν υπό τη διαχείρισή του

2.1.2 Προσωπικές συσκευές που έχουν εγκριθεί βάσει της πολιτικής Χρήσης Προσωπικών Συσκευών (BYOD), υπό την προϋπόθεση εγκατάστασης MDM ή πράκτορα τερματικού σημείου

2.1.3 Διακομιστές και περιουσιακά στοιχεία υποδομής, συμπεριλαμβανομένων εικονικών μηχανών που φιλοξενούνται σε περιβάλλον νέφους και συσκευών ακμής

2.1.4 Λειτουργικά συστήματα, οδηγοί, τοπικές υπηρεσίες, πράκτορες τερματικών σημείων και έλεγχοι ασφάλειας που είναι εγκατεστημένοι σε κάθε κόμβο

2.2 Όλο το προσωπικό με διοικητική, τεχνική ή επιχειρησιακή ευθύνη για οποιοδήποτε τερματικό σημείο υπάγεται στην παρούσα πολιτική, συμπεριλαμβανομένων των εξής:

2.2.1 Εσωτερικοί εργαζόμενοι και ανάδοχοι

2.2.2 Πάροχοι διαχειριζόμενων υπηρεσιών (MSPs), εξωτερικές υπηρεσίες υποστήριξης επιτραπέζιων συστημάτων και διαχειριστές ΤΠ τρίτων μερών

2.2.3 Χρήστες που έχουν εξουσιοδοτηθεί να χρησιμοποιούν φορητά συστήματα, φορητούς υπολογιστές με δυνατότητα VPN ή φορητή πρόσβαση σε δίκτυα του οργανισμού

2.3 Η κάλυψη απειλών βάσει της παρούσας πολιτικής περιλαμβάνει, ενδεικτικά και όχι περιοριστικά, τα εξής:

2.3.1 Ιούς, worms, trojans, ransomware, spyware, rootkits, adware, καταγραφείς πληκτρολογήσεων, botnets

2.3.2 Κακόβουλο λογισμικό χωρίς αρχεία, zero-day payloads, κακόβουλο λογισμικό κλιμάκωσης προνομίων και εργαλειοθήκες εκμετάλλευσης προγραμμάτων περιήγησης

2.3.3 Κακόβουλο κώδικα που μεταδίδεται μέσω αφαιρούμενων μέσων, εκστρατειών ηλεκτρονικού ψαρέματος, drive-by downloads ή επιθέσεων μέσω USB

3. Στόχοι

3.1 Να προστατεύεται η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα των τερματικών σημείων και των δεδομένων που αυτά επεξεργάζονται, μέσω αξιόπιστης πρόληψης, ανίχνευσης και απόκρισης έναντι κακόβουλου λογισμικού.

3.2 Να αποτρέπεται η εκτέλεση ή η διάδοση κακόβουλου κώδικα στα δίκτυα του οργανισμού, με την εφαρμογή τεχνικών δικλίδων ασφαλείας, σκλήρυνσης βασικών γραμμών και τηλεμετρίας σε πραγματικό χρόνο.

3.3 Να ενσωματώνεται η προστασία τερματικών σημείων με άλλους ελέγχους του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS), συμπεριλαμβανομένων της διαχείρισης ευπαθειών, του ελέγχου πρόσβασης, της καταγραφής ελέγχου και παρακολούθησης και της απόκρισης σε περιστατικά.

3.4 Να διασφαλίζεται συνεχής ορατότητα των τερματικών σημείων μέσω κεντρικά διαχειριζόμενων πλατφορμών προστασίας, συμπεριλαμβανομένων πρακτόρων αντιιικού/αντικακόβουλου λογισμικού, Ανίχνευσης και Απόκρισης Τερματικών Σημείων (EDR) και τηλεμετρίας SIEM.

3.5 Να τηρούνται οι νομικές, κανονιστικές και προτυποποιημένες απαιτήσεις που επιβάλλουν ασφάλεια τερματικών σημείων, όπως το Άρθρο 32 του ΓΚΠΔ της ΕΕ, το Άρθρο 21 της Οδηγίας NIS2 της ΕΕ και το Άρθρο 9 του Κανονισμού DORA της ΕΕ.

3.6 Να καθορίζονται σαφώς οι υπόλογοι ρόλοι, να εφαρμόζονται συμφωνίες επιπέδου υπηρεσιών (SLA) για την εφαρμογή διορθώσεων και την απόκριση σε ειδοποιήσεις, και να διασφαλίζεται ετοιμότητα ελέγχου μέσω τεκμηρίωσης και αναφοράς.

4. Ρόλοι και αρμοδιότητες

4.1 Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1 Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει την ευθυγράμμισή της με το ISMS και τη συνολική στρατηγική ασφάλειας.

4.1.2 Ανασκοπεί σε τριμηνιαία βάση τις μετρικές προστασίας τερματικών σημείων, τις τάσεις περιστατικών και την αποτελεσματικότητα των εργαλείων.

4.1.3 Εγκρίνει εξαιρέσεις και αποδοχές υπολειπόμενου κινδύνου που σχετίζονται με την κάλυψη τερματικών σημείων.

4.2 Επικεφαλής Ασφάλειας Τερματικών Σημείων / Διευθυντής SOC

4.2.1 Διαχειρίζεται τα συστήματα προστασίας τερματικών σημείων, όπως AV, EDR και MDM.

4.2.2 Ασκεί εποπτεία στην εφαρμογή της πολιτικής, στη ρύθμιση της ανίχνευσης απειλών και στα εγχειρίδια ενεργειών απόκρισης.

4.2.3 Τηρεί στατιστικά κάλυψης, αρχεία καταγραφής περιστατικών κακόβουλου λογισμικού και βασικές γραμμές ρυθμίσεων ειδοποιήσεων.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Απαιτήσεις ανασκόπησης και επικαιροποίησης

9.1 Η παρούσα πολιτική πρέπει να ανασκοπείται ετησίως ή όταν:

9.1.1 Σημειώνονται μείζονες εκστρατείες κακόβουλου λογισμικού ή περιστατικά ασφάλειας τερματικών σημείων

9.1.2 Νέοι τύποι απειλών, όπως κακόβουλο λογισμικό χωρίς αρχεία ή παραλλαγές ransomware, απαιτούν επικαιροποιημένες στρατηγικές ανίχνευσης ή απόκρισης

9.1.3 Οι πλατφόρμες προστασίας τερματικών σημείων ή οι αρχιτεκτονικές πρακτόρων μεταβάλλονται σημαντικά

9.1.4 Επικαιροποιούνται νομικές ή κανονιστικές απαιτήσεις που επηρεάζουν τους ελέγχους τερματικών σημείων

9.2 Η ανασκόπηση πρέπει να εκκινείται από τον Επικεφαλής Ασφάλειας Τερματικών Σημείων και να συντονίζεται με τις λειτουργίες Ασφάλειας Πληροφοριών, Νομικής Υπηρεσίας, Διαχείρισης Κινδύνων και Ελέγχου.

9.3 Οι εγκεκριμένες αναθεωρήσεις πρέπει να τεκμηριώνονται στο Μητρώο Εγγράφων ISMS, να λαμβάνουν νέο αναγνωριστικό έκδοσης και να κοινοποιούνται σε όλα τα επηρεαζόμενα μέρη.

9.4 Οι καταργημένες εκδόσεις πρέπει να αρχειοθετούνται, να υπόκεινται σε περιορισμό πρόσβασης και να διατηρούνται για τη διασφάλιση της ακεραιότητας του ίχνους ελέγχου, σύμφωνα με τα χρονοδιαγράμματα διατήρησης του ISMS.

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 P1 - Πολιτική Ασφάλειας Πληροφοριών. Καθορίζει τις θεμελιώδεις αρχές για την προστασία συστημάτων, δεδομένων και δικτύων. Η παρούσα πολιτική εφαρμόζει τις αρχές αυτές στο επίπεδο του τερματικού σημείου μέσω τεχνικών και διαδικαστικών ελέγχων κατά του κακόβουλου λογισμικού.

10.2 P4 - Πολιτική Ελέγχου Πρόσβασης. Ορίζει περιορισμούς πρόσβασης χρηστών, οι οποίοι εφαρμόζονται στο επίπεδο του τερματικού σημείου, συμπεριλαμβανομένων ελέγχων κατά της κλιμάκωσης προνομίων και της μη εξουσιοδοτημένης εγκατάστασης μη αξιολογημένου λογισμικού.

10.3 P5 - Πολιτική Διαχείρισης Αλλαγών. Διασφαλίζει ότι οι επικαιροποιήσεις στο λογισμικό προστασίας τερματικών σημείων, στους κανόνες πολιτικής ή στις παραμετροποιήσεις πρακτόρων υπόκεινται σε έγκριση και ελεγχόμενες διαδικασίες εγκατάστασης.

10.4 P12 - Πολιτική Διαχείρισης Περιουσιακών Στοιχείων. Παρέχει τη βασική γραμμή ταξινόμησης περιουσιακών στοιχείων και απογραφής που απαιτείται για την ορατότητα τερματικών σημείων, την κάλυψη επιδιόρθωσης και τον ορισμό του πεδίου εφαρμογής της προστασίας από κακόβουλο λογισμικό.

10.5 P22 - Πολιτική Καταγραφής και Παρακολούθησης. Επιτρέπει την ενοποίηση ειδοποιήσεων τερματικών σημείων, της κατάστασης υγείας πρακτόρων και της πληροφόρησης απειλών σε κεντρικά συστήματα SIEM για ανίχνευση σε πραγματικό χρόνο και εγκληματολογική ιχνηλασιμότητα.

10.6 P30 - Πολιτική Αντιμετώπισης Περιστατικών (P30). Συνδέει περιστατικά κακόβουλου λογισμικού που προέρχονται από τερματικά σημεία με τυποποιημένες ροές εργασιών περιορισμού, εξάλειψης, διερεύνησης και ανάκαμψης, με καθορισμένους ρόλους και κατώφλια κλιμάκωσης.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001:

11.1.1 Ρήτρα 8.1 - Επιχειρησιακός σχεδιασμός και έλεγχος: Απαιτεί την εφαρμογή τεχνικών ελέγχων, συμπεριλαμβανομένων δικλίδων προστασίας τερματικών σημείων, για τη διατήρηση των στόχων του ISMS.

11.2 ISO/IEC 27002:2022 - Έλεγχοι 8.7, 8:

11.2.1 Παρέχει αναλυτική τεχνική καθοδήγηση για μέτρα κατά του κακόβουλου λογισμικού, ασφαλή εγκατάσταση λογισμικού, παρακολούθηση και ετοιμότητα αντιμετώπισης περιστατικών για περιβάλλοντα τερματικών σημείων.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Προστασία από κακόβουλο κώδικα: Απαιτεί τη χρήση εργαλείων κατά του κακόβουλου λογισμικού με σάρωση σε πραγματικό χρόνο, προστασία κατά την πρόσβαση και ανάλυση συμπεριφοράς.

11.3.2 SI-4 - Παρακολούθηση συστημάτων: Υποστηρίζει την ενοποίηση τηλεμετρίας με κεντρικές πλατφόρμες ανίχνευσης.

11.3.3 CM-6 - Ρυθμίσεις παραμέτρων: Ενισχύει τις βασικές ρυθμίσεις ελέγχου στα τερματικά σημεία, συμπεριλαμβανομένης της εφαρμογής πρακτόρων προστασίας.

11.4 ΓΚΠΔ της ΕΕ (2016/679):

11.4.1 Άρθρο 32 - Ασφάλεια της επεξεργασίας: Απαιτεί από τους οργανισμούς να εφαρμόζουν κατάλληλα τεχνικά μέτρα για τη διασφάλιση των προσωπικών δεδομένων, συμπεριλαμβανομένης της προστασίας από απειλές κακόβουλου λογισμικού.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555):

11.5.1 Άρθρο 21(2)(d): Υποχρεώνει τις οντότητες να εφαρμόζουν μέτρα ανίχνευσης και πρόληψης απειλών, συμπεριλαμβανομένων μηχανισμών άμυνας κατά του κακόβουλου λογισμικού σε επίπεδο τερματικού σημείου.

11.6 Κανονισμός DORA της ΕΕ (2022/2554):

11.6.1 Άρθρο 9 - Απαιτήσεις διαχείρισης κινδύνων ΤΠΕ: Απαιτεί από τις χρηματοοικονομικές οντότητες να υιοθετούν προστατευτικά μέτρα για την πρόληψη, ανίχνευση και απόκριση έναντι κακόβουλου λογισμικού και απειλών που προέρχονται από τερματικά σημεία.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Προστασία από κακόβουλο λογισμικό: Απαιτεί την ανίχνευση και τον μετριασμό κακόβουλου λογισμικού σε όλα τα τερματικά σημεία του οργανισμού.

11.7.2 DSS01.04 - Διαχείριση διαθεσιμότητας και χωρητικότητας: Διασφαλίζει ότι η προστασία από κακόβουλο λογισμικό εξισορροπείται με την απόδοση των συστημάτων και την επιχειρησιακή συνέχεια.

11.7.3 MEA03 - Παρακολούθηση, αξιολόγηση και εκτίμηση της συμμόρφωσης: Απαιτεί περιοδικό έλεγχο των ελέγχων τερματικών σημείων και της αποτελεσματικότητας της προστασίας.