					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P20S					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	Clause 8	Επιχειρησιακοί έλεγχοι για προστασία από κακόβουλο λογισμικό
ISO/IEC 27002:2022	Control 8	Μέτρα ελέγχου για την προστασία τερματικών σημείων
NIST SP 800-53 Rev.5	SI-3, SI-4	Προστασία από κακόβουλο κώδικα και απόκριση σε περιστατικά
Οδηγία NIS2 της ΕΕ	Articles 21(2)(d), (e)	Διαχείριση κακόβουλου λογισμικού και κινδύνων για ουσιώδεις και σημαντικές οντότητες
Κανονισμός DORA της ΕΕ	Articles 10(1), 15	Λειτουργική ανθεκτικότητα και επαλήθευση τρίτων μερών
COBIT 2019	DSS05.02, DSS05.04	Προστασία τερματικών σημείων/δικτύου και παρακολούθηση
ΓΚΠΔ της ΕΕ	Articles 32(1)(b), 33	Τεχνικά και οργανωτικά μέτρα και κοινοποίηση παραβίασης

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τις ελάχιστες τεχνικές, διαδικαστικές και συμπεριφορικές απαιτήσεις για την προστασία όλων των συσκευών τελικού σημείου — όπως φορητοί υπολογιστές, επιτραπέζιοι υπολογιστές, κινητές συσκευές και φορητά μέσα αποθήκευσης — από κακόβουλο κώδικα, συμπεριλαμβανομένων ιών, ransomware, spyware, rootkits και άλλων απειλών κακόβουλου λογισμικού.

1.2 Σκοπός της είναι να διασφαλίζει ότι τα τελικά σημεία εξοπλίζονται, συντηρούνται και χρησιμοποιούνται κατά τρόπο που μειώνει τον κίνδυνο μόλυνσης από κακόβουλο λογισμικό, εξάπλωσής του και παραβίασης συστημάτων.

1.3 Ο οργανισμός αναγνωρίζει ότι τα τελικά σημεία αποτελούν συνήθη σημεία εισόδου κακόβουλου λογισμικού και, ως εκ τούτου, πρέπει να υποβάλλονται σε σκλήρυνση, να παρακολουθούνται και να προστατεύονται με άμυνα σε βάθος.

1.4 Η πολιτική υποστηρίζει τους στόχους πιστοποίησης του οργανισμού κατά ISO/IEC 27001:2022 και ευθυγραμμίζεται με τον ΓΚΠΔ της ΕΕ, την Οδηγία NIS2 της ΕΕ, τον Κανονισμό DORA της ΕΕ και άλλα συναφή πλαίσια.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται στα εξής:

2.1.1 Όλα τα τελικά σημεία του οργανισμού, συμπεριλαμβανομένων επιτραπέζιων υπολογιστών, φορητών υπολογιστών, tablets, κινητών τηλεφώνων και τερματικών σημείων πώλησης

2.1.2 Προσωπικές συσκευές (BYOD) που χρησιμοποιούνται για πρόσβαση σε επιχειρησιακές εφαρμογές ή δεδομένα

2.1.3 Αφαιρούμενα μέσα αποθήκευσης, όπως μονάδες USB και εξωτερικοί σκληροί δίσκοι

2.1.4 Οποιαδήποτε λειτουργικά συστήματα, λογισμικό τελικών σημείων ή εργαλεία επικοινωνίας εκτελούνται στις ανωτέρω πλατφόρμες

2.2 Εφαρμόζεται εξίσου στα εξής:

2.2.1 Εσωτερικό προσωπικό, ανάδοχοι, ασκούμενοι και πάροχοι διαχειριζόμενων υπηρεσιών (MSPs)

2.2.2 Συσκευές που χρησιμοποιούνται εντός εγκαταστάσεων, απομακρυσμένα ή στο πλαίσιο υβριδικών ρυθμίσεων εργασίας

2.2.3 Τελικά σημεία συνδεδεμένα με το υπολογιστικό νέφος ή εκτός σύνδεσης που αποθηκεύουν επιχειρησιακά ή προσωπικά δεδομένα

3. Στόχοι

3.1 Πρόληψη μόλυνσης από κακόβουλο λογισμικό και εξάπλωσής του στα εσωτερικά συστήματα, στις συσκευές χρηστών και στις εξωτερικές συνδέσεις

3.2 Έγκαιρη ανίχνευση και περιορισμός απειλών που σχετίζονται με κακόβουλο λογισμικό με τη χρήση αυτοματοποιημένων τεχνολογιών ασφάλειας τελικών σημείων και καθορισμένων διαδρομών κλιμάκωσης

3.3 Διασφάλιση ότι μόνο εξουσιοδοτημένες, ασφαλείς και παρακολουθούμενες συσκευές χρησιμοποιούνται για πρόσβαση σε επιχειρησιακές πληροφορίες

3.4 Καθιέρωση σαφών αρμοδιοτήτων του προσωπικού και κανόνων συμπεριφοράς των χρηστών για τη μείωση του κινδύνου περιστατικών που σχετίζονται με κακόβουλο λογισμικό

3.5 Τήρηση ιχνηλάσιμων και ελέγξιμων αρχείων για ανιχνεύσεις κακόβουλου λογισμικού, ενέργειες απόκρισης και συμμόρφωση με την πολιτική

3.6 Προστασία προσωπικών και επιχειρησιακών δεδομένων από παραβίαση λόγω κακόβουλου λογισμικού με χρήση στρατηγικών άμυνας σε βάθος

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Είναι ο ιδιοκτήτης της παρούσας πολιτικής και διασφαλίζει τη διάθεση επαρκών πόρων για την προστασία των τελικών σημείων

4.1.2 Εγκρίνει το λογισμικό προστασίας από ιούς, τα εργαλεία διαχείρισης φορητών συσκευών (MDM) και τους κανόνες πρόσβασης τρίτων μερών

4.1.3 Ανασκοπεί αναφορές περιστατικών κακόβουλου λογισμικού, συνόψεις αντικτύπου και κοινοποιήσεις παραβίασης που αφορούν τελικά σημεία

4.2 Εξωτερικός πάροχος υπηρεσιών πληροφορικής / διαχειριστής Πληροφορικής

4.2.1 Επιλέγει και εγκαθιστά λογισμικό προστασίας από ιούς, λογισμικό anti-malware και λύσεις Ανίχνευσης και Απόκρισης Τερματικών Σημείων (EDR)

4.2.2 Διασφαλίζει ότι οι ενημερώσεις εφαρμόζονται με συνέπεια και ότι τα αρχεία καταγραφής διατηρούνται

4.2.3 Ανταποκρίνεται σε ειδοποιήσεις κακόβουλου λογισμικού, απομονώνει μολυσμένα συστήματα και υλοποιεί ενέργειες αποκατάστασης

4.2.4 Εφαρμόζει ελέγχους για τη χρήση USB και εξωτερικών συσκευών

[... 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 Απαίτηση ετήσιας ανασκόπησης

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται επίσημα τουλάχιστον μία φορά κατ' έτος από τον Γενικό Διευθυντή, σε συντονισμό με τον Εξωτερικό πάροχο υπηρεσιών πληροφορικής και τον Συντονιστή Ιδιωτικότητας

9.2 Επικαιροποιήσεις βάσει εναυσμάτων

9.2.1 Η επικαιροποίηση της πολιτικής πρέπει επίσης να πραγματοποιείται όταν:

9.2.1.1 Μια σημαντική νέα απειλή κακόβουλου λογισμικού ή έξαρση στοχεύει τελικά σημεία που χρησιμοποιεί ο οργανισμός

9.2.1.2 Τα εργαλεία λογισμικού προστασίας από ιούς ή EDR αλλάζουν, αναβαθμίζονται ή αντικαθίστανται

9.2.1.3 Ένα περιστατικό κακόβουλου λογισμικού αποκαλύπτει αδυναμίες στο πεδίο εφαρμογής ή στην εφαρμογή της παρούσας πολιτικής

9.2.1.4 Νομικές ή κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ, Οδηγία NIS2 της ΕΕ) επικαιροποιούνται

9.3 Έλεγχος εκδόσεων και επικοινωνία

9.3.1 Όλες οι αλλαγές της πολιτικής πρέπει να τεκμηριώνονται με αριθμό έκδοσης, ημερομηνία και σύνοψη αλλαγών

9.3.2 Το προσωπικό πρέπει να ενημερώνεται για τις επικαιροποιήσεις, ιδίως εάν μεταβάλλουν επιχειρησιακές ή συμπεριφορικές απαιτήσεις

9.3.3 Οι προηγούμενες εκδόσεις πρέπει να διατηρούνται στο αρχείο πολιτικών για τουλάχιστον 3 έτη προς υποστήριξη ελέγχων

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συνδυασμό με τις ακόλουθες πολιτικές SME:

10.1.1 P9S – Πολιτική Τηλεργασίας: Διασφαλίζει ότι οι απαιτήσεις προστασίας τελικών σημείων εφαρμόζονται σε συσκευές που χρησιμοποιούνται εκτός εγκαταστάσεων ή σε υβριδικά περιβάλλοντα

10.1.2 P12S – Πολιτική Διαχείρισης Περιουσιακών Στοιχείων: Υποστηρίζει την παρακολούθηση και τον έλεγχο όλων των τελικών σημείων, διασφαλίζοντας ότι χρησιμοποιούνται μόνο εξουσιοδοτημένες και προστατευμένες συσκευές

10.1.3 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Ενισχύει την πρόληψη κακόβουλου λογισμικού ως βασικό έλεγχο ιδιωτικότητας για την προστασία προσωπικών και ευαίσθητων δεδομένων από παραβίαση

10.1.4 P22S – Πολιτική Καταγραφής και Παρακολούθησης: Καθορίζει τις απαιτήσεις για την καταγραφή συμβάντων κακόβουλου λογισμικού και τη διατήρηση ορατότητας ειδοποιήσεων για έγκαιρη απόκριση

10.1.5 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Καθορίζει τα βήματα κλιμάκωσης, περιορισμού και εξωτερικής κοινοποίησης εάν κακόβουλο λογισμικό οδηγήσει σε παραβίαση δεδομένων ή επιχειρησιακή διαταραχή

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Απαιτεί την εφαρμογή επιχειρησιακών ελέγχων για τη μείωση κινδύνων όπως οι επιθέσεις κακόβουλου λογισμικού

11.2 ISO/IEC 27002

11.2.1 Control 8.7 – Περιγράφει πρακτικές ελέγχου κακόβουλου λογισμικού, συμπεριλαμβανομένων λογισμικού προστασίας από ιούς, σάρωσης σε πραγματικό χρόνο, ενημερώσεων και εκπαίδευσης χρηστών

11.3 NIST SP 800-53 Rev.5

11.3.1 SI-3 – Απαιτεί την εγκατάσταση μηχανισμών προστασίας από κακόβουλο κώδικα σε όλα τα τελικά σημεία

11.3.2 SI-4 – Επιβάλλει ενέργειες παρακολούθησης, ανίχνευσης, ανάλυσης και απόκρισης για απειλές και ειδοποιήσεις σε επίπεδο τελικού σημείου

11.4 ΓΚΠΔ της ΕΕ

11.4.1 Article 32(1)(b) – Απαιτεί τεχνικούς και οργανωτικούς ελέγχους (όπως λογισμικό προστασίας από ιούς) για την προστασία προσωπικών δεδομένων

11.4.2 Article 33 – Επιβάλλει κοινοποίηση παραβίασης όταν κακόβουλο λογισμικό θίγει την ακεραιότητα, εμπιστευτικότητα ή διαθεσιμότητα δεδομένων

11.5 Οδηγία NIS2 της ΕΕ

11.5.1 Article 21(2)(d) – Απαιτεί μέτρα για την πρόληψη και την απόκριση σε απειλές κακόβουλου λογισμικού εντός ουσιωδών και σημαντικών οντοτήτων

11.5.2 Article 21(2)(e) – Επιβάλλει πολυεπίπεδες στρατηγικές διαχείρισης κινδύνων κυβερνοασφάλειας, συμπεριλαμβανομένης της προστασίας τελικών σημείων από κακόβουλο λογισμικό

11.6 Κανονισμός DORA της ΕΕ

11.6.1 Article 10(1) – Απαιτεί τα συστήματα ΤΠΕ να προστατεύονται από κακόβουλο λογισμικό και άλλες απειλές στο πλαίσιο της λειτουργικής ανθεκτικότητας

11.6.2 Article 15 – Επιβάλλει στους χρηματοπιστωτικούς οργανισμούς να επαληθεύουν την προστασία από κακόβουλο λογισμικό στους τρίτους παρόχους υπηρεσιών

11.7 COBIT 2019

11.7.1 DSS05.02 – Δίνει έμφαση σε προστατευτικά μέτρα για την άμυνα τελικών σημείων και δικτύων έναντι απειλών κακόβουλου λογισμικού

11.7.2 DSS05.04 – Υποστηρίζει την παρακολούθηση και τις ειδοποιήσεις για συμβάντα ασφάλειας που σχετίζονται με κακόβουλο λογισμικό στο πλαίσιο των συνεχιζόμενων λειτουργιών