					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P29S					Τίτλος εγγράφου: **Πολιτική Δεδομένων Δοκιμών και Περιβαλλόντων Δοκιμών**							
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	Ρήτρες 6.1, 8	
ISO/IEC 27002:2022	Έλεγχοι 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
ΓΚΠΔ της ΕΕ	Άρθρα 5(1)(c), 25, 32	
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e), (h)	
Κανονισμός DORA της ΕΕ	Άρθρο 9	
COBIT 2019	BAI07, DSS05	

1. Σκοπός

1.1 Η παρούσα πολιτική καθορίζει τον τρόπο διαχείρισης των δεδομένων δοκιμών και των περιβαλλόντων δοκιμών, ώστε να αποτρέπεται η ακούσια έκθεση, η παραβίαση δεδομένων ή η επιχειρησιακή διαταραχή κατά τη διάρκεια δραστηριοτήτων δοκιμών.

1.2 Διασφαλίζει ότι πραγματικά δεδομένα πελατών δεν χρησιμοποιούνται ακατάλληλα κατά τις δοκιμές λογισμικού ή συστημάτων και ότι τα περιβάλλοντα δοκιμών είναι λογικά και τεχνικά διαχωρισμένα από τα συστήματα παραγωγής.

1.3 Η πολιτική έχει σχεδιαστεί ώστε να βοηθά τις ΜΜΕ να συμμορφώνονται με τις απαιτήσεις πιστοποίησης ISO/IEC 27001 και τη σχετική νομοθεσία για την προστασία δεδομένων, παραμένοντας παράλληλα πρακτική και εφαρμόσιμη για οργανισμούς χωρίς εξειδικευμένη ομάδα Πληροφορικής.

2. Πεδίο εφαρμογής

2.1 Η παρούσα πολιτική εφαρμόζεται σε:

2.1.1 Όλα τα περιβάλλοντα δοκιμών (π.χ. περιβάλλοντα σταδιοποίησης, απομονωμένα περιβάλλοντα δοκιμών, δοκιμαστικά περιβάλλοντα ανάπτυξης)

2.1.2 Όλα τα δεδομένα δοκιμών, είτε δημιουργούνται χειροκίνητα, είτε παράγονται συνθετικά, είτε προέρχονται από ενεργά δεδομένα

2.1.3 Όλο το προσωπικό που συμμετέχει σε δραστηριότητες δοκιμών, συμπεριλαμβανομένων εργαζομένων, αναδόχων, ελεύθερων επαγγελματιών και παρόχων υπηρεσιών Πληροφορικής

2.1.4 Κάθε δοκιμή που μπορεί να επηρεάσει πλατφόρμες προσβάσιμες από πελάτες, εσωτερικά επιχειρησιακά συστήματα ή υπηρεσίες τρίτων

2.2 Καλύπτει τόσο τα τεχνικά περιβάλλοντα όσο και τις διαδικασίες που χρησιμοποιούνται για την υποστήριξη:

2.2.1 Της ανάπτυξης ιστοτόπων, εφαρμογών και εργαλείων

2.2.2 Αναβαθμίσεων συστημάτων, δοκιμών παραμετροποίησης και δοκιμών ολοκλήρωσης

2.2.3 Αυτοματοποιημένων και χειροκίνητων λειτουργικών δοκιμών ή δοκιμών ασφάλειας

3. Στόχοι

3.1 Να αποτρέπεται η χρήση πραγματικών, ταυτοποιήσιμων δεδομένων πελατών σε δοκιμές, εκτός εάν έχουν ανωνυμοποιηθεί και εγκριθεί ρητά.

3.2 Να διατηρείται αυστηρός διαχωρισμός μεταξύ συστημάτων δοκιμών και συστημάτων παραγωγής, ώστε να αποφεύγεται η ακούσια έκθεση δεδομένων ή η επιχειρησιακή παρεμβολή.

3.3 Να προστατεύονται τα συστήματα και τα δεδομένα δοκιμών από μη εξουσιοδοτημένη πρόσβαση, ακούσια γνωστοποίηση ή επαναχρησιμοποίηση μεταξύ περιβαλλόντων χωρίς κατάλληλες δικλίδες ασφαλείας.

3.4 Να διασφαλίζεται η συμμόρφωση με τις σχετικές κανονιστικές απαιτήσεις για την προστασία δεδομένων (π.χ. ΓΚΠΔ της ΕΕ, Οδηγία NIS2 της ΕΕ), με διασφάλιση ότι όλα τα δεδομένα δοκιμών υποβάλλονται σε νόμιμη, θεμιτή και ασφαλή επεξεργασία.

3.5 Να υποστηρίζεται η ετοιμότητα του οργανισμού για εξωτερικό έλεγχο και πιστοποίηση ISO/IEC 27001, μέσω τεκμηρίωσης των πρακτικών δοκιμών και εφαρμογής συνεπών δικλίδων ασφαλείας.

4. Ρόλοι και αρμοδιότητες

4.1 Γενικός Διευθυντής (GM)

4.1.1 Έχει τη συνολική λογοδοσία για την προστασία των δεδομένων δοκιμών και την ασφάλεια των συστημάτων δοκιμών.

4.1.2 Εγκρίνει κάθε χρήση πραγματικών δεδομένων σε δοκιμές, αφού επιβεβαιώσει ότι εφαρμόζονται κατάλληλες δικλίδες ασφαλείας (π.χ. ανωνυμοποίηση ή απόκρυψη δεδομένων).

4.1.3 Επαληθεύει ότι οι δραστηριότητες δοκιμών τεκμηριώνονται επαρκώς και συμμορφώνονται με την παρούσα πολιτική.

4.2 Ιδιοκτήτης έργου

4.2.1 Συντονίζει τον σχεδιασμό και την εκτέλεση των διαδικασιών δοκιμών.

4.2.2 Διασφαλίζει ότι όλα τα μέλη της ομάδας κατανοούν και τηρούν την παρούσα πολιτική.

4.2.3 Επιβεβαιώνει ότι τα συστήματα δοκιμών έχουν διαμορφωθεί με ασφαλή τρόπο πριν από την έναρξη των δοκιμών.

4.2.4 Αναφέρει στον GM κάθε περιστατικό που αφορά περιβάλλοντα δοκιμών ή διαρροή δεδομένων.

[... 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 Προγραμματισμένες ανασκοπήσεις

9.1.1 Η παρούσα πολιτική πρέπει να ανασκοπείται τουλάχιστον μία φορά ετησίως από τον Γενικό Διευθυντή (GM). Η ανασκόπηση διασφαλίζει ότι η πολιτική παραμένει επίκαιρη ως προς:

9.1.1.1 Τις αλλαγές σε εργαλεία, πλατφόρμες ή περιβάλλοντα ανάπτυξης λογισμικού

9.1.1.2 Τις επικαιροποιημένες νομικές υποχρεώσεις, συμπεριλαμβανομένων απαιτήσεων για την προστασία δεδομένων ή την ψηφιακή ανθεκτικότητα

9.1.1.3 Την πιστοποίηση ΜΜΕ και την ετοιμότητα για έλεγχο σύμφωνα με το ISO/IEC 27001

9.2 Γεγονότα ενεργοποίησης ενδιάμεσης ανασκόπησης

9.2.1 Πρόσθετες ανασκοπήσεις πρέπει να πραγματοποιούνται κατόπιν:

9.2.1.1 Οποιουδήποτε περιστατικού που περιλαμβάνει έκθεση δεδομένων ή παραβίαση σε περιβάλλοντα δοκιμών

9.2.1.2 Χρήσης πραγματικών δεδομένων σε δοκιμές, ακόμη και εάν έχουν ανωνυμοποιηθεί

9.2.1.3 Εισαγωγής νέων μεθόδων δοκιμών, συστημάτων ή προμηθευτών

9.2.1.4 Κανονιστικών επικαιροποιήσεων που επηρεάζουν τον τρόπο χειρισμού δεδομένων κατά τις δοκιμές

9.3 Διαχείριση αλλαγών και επικοινωνία

9.3.1 Ο GM είναι υπεύθυνος για:

9.3.1.1 Την επικαιροποίηση της παρούσας πολιτικής και την τεκμηρίωση κάθε αναθεώρησης στο ιστορικό εκδόσεων

9.3.1.2 Την ενημέρωση του προσωπικού, των προγραμματιστών και των σχετικών παρόχων υπηρεσιών για τις επικαιροποιήσεις

9.3.1.3 Την επιβεβαίωση ότι όλο το προσωπικό που σχετίζεται με δοκιμές κατανοεί και εφαρμόζει τους πλέον πρόσφατους κανόνες

9.3.1.4 Τη διατήρηση προσβάσιμης έκδοσης της πλέον πρόσφατης πολιτικής για σκοπούς ανασκόπησης και ελέγχου

9.4 Έλεγχος και τεκμηρίωση

9.4.1 Τα αρχεία όλων των ανασκοπήσεων της πολιτικής, των εγκρίσεων χρήσης πραγματικών δεδομένων και κάθε αιτιολόγησης εξαίρεσης πρέπει:

9.4.1.1 Να διατηρούνται με ασφάλεια για σκοπούς ελέγχου

9.4.1.2 Να είναι διαθέσιμα κατόπιν αιτήματος κατά τη διάρκεια εσωτερικών ελέγχων ή ελέγχων τρίτων

9.4.1.3 Να ανασκοπούνται ετησίως ώστε να διασφαλίζεται η συνέπεια με τις πρακτικές δοκιμών

10. Συναφείς πολιτικές και διασυνδέσεις

10.1 Η παρούσα πολιτική πρέπει να εφαρμόζεται σε συντονισμό με τις ακόλουθες πολιτικές ΜΜΕ, ώστε να διατηρούνται η ασφάλεια και η συμμόρφωση κατά τις δοκιμές:

10.1.1 P2S – Πολιτική Ρόλων και Αρμοδιοτήτων Διακυβέρνησης: Καθορίζει ποιος λογοδοτεί για την εποπτεία της ανάπτυξης, των δοκιμών και των αρμοδιοτήτων διαχωρισμού συστημάτων.

10.1.2 P4S – Πολιτική Ελέγχου Πρόσβασης: Διέπει την ανάθεση, τη διαχείριση και την αφαίρεση διαπιστευτηρίων πρόσβασης στα συστήματα δοκιμών.

10.1.3 P8S – Πολιτική Ευαισθητοποίησης και Εκπαίδευσης για την Ασφάλεια Πληροφοριών: Διασφαλίζει ότι το προσωπικό κατανοεί τους κινδύνους των δεδομένων δοκιμών, τις ασφαλείς πρακτικές χειρισμού και τον ορθό διαχωρισμό περιβαλλόντων.

10.1.4 P13S – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Υποστηρίζει τη σαφή ταξινόμηση των δεδομένων δοκιμών και καθοδηγεί τις στρατηγικές ανωνυμοποίησης ή απόκρυψης δεδομένων.

10.1.5 P17S – Πολιτική Προστασίας Δεδομένων και Ιδιωτικότητας: Ευθυγραμμίζεται με τις υποχρεώσεις του ΓΚΠΔ της ΕΕ, συμπεριλαμβανομένων των δικλίδων ασφαλείας για την επεξεργασία και αποθήκευση δεδομένων προσωπικού χαρακτήρα, ακόμη και σε περιβάλλοντα δοκιμών.

10.1.6 P24S – Πολιτική Ασφαλούς Ανάπτυξης: Παρέχει τις συνολικές απαιτήσεις ασφάλειας για τις ομάδες ανάπτυξης, συμπεριλαμβανομένης της ασφαλούς χρήσης δεδομένων κατά τις φάσεις δοκιμών.

10.1.7 P30S – Πολιτική Αντιμετώπισης Περιστατικών: Περιγράφει τον τρόπο απόκρισης σε οποιαδήποτε παραβίαση ή ζήτημα εντοπίζεται σε περιβάλλον δοκιμών ή προκαλείται από ακατάλληλο χειρισμό δεδομένων δοκιμών.

10.2 Οι πολιτικές αυτές συνθέτουν ένα ενιαίο πλαίσιο ασφάλειας που υποστηρίζει την ακεραιότητα των δοκιμών, την ελαχιστοποίηση δεδομένων και την πλήρη ευθυγράμμιση με το ISO/IEC 27001 σε όλες τις λειτουργίες ανάπτυξης και διασφάλισης ποιότητας.

11. Πρότυπα και πλαίσια αναφοράς

11.1 ISO/IEC 27001

11.1.1 Ρήτρα 6.1 – Απαιτεί αξιολόγηση κινδύνων και ενέργειες αντιμετώπισης, συμπεριλαμβανομένων κινδύνων που σχετίζονται με δοκιμές.

11.1.2 Ρήτρα 8.1 – Απαιτεί προγραμματισμό και έλεγχο των επιχειρησιακών διεργασιών, συμπεριλαμβανομένων των περιβαλλόντων εγκατάστασης συστημάτων δοκιμών.

11.2 ISO/IEC 27002

11.2.1 Έλεγχος 8.28 – Απαιτεί από τους οργανισμούς να προστατεύουν τα δεδομένα δοκιμών και να διασφαλίζουν ότι δεν περιέχουν ευαίσθητα δεδομένα ή ενεργά δεδομένα παραγωγής.

11.2.2 Έλεγχος 8.29 – Επιβάλλει σαφή διαχωρισμό μεταξύ περιβαλλόντων ανάπτυξης, δοκιμών και παραγωγής.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Καλύπτει τις απαιτήσεις ελέγχου για την ανάπτυξη και τις δοκιμές.

11.3.2 SA-12 – Αντιμετωπίζει τους κινδύνους δοκιμών στην εφοδιαστική αλυσίδα και τις αξιολογήσεις ασφάλειας.

11.3.3 SC-32 – Απαιτεί διαχωρισμό περιβαλλόντων και προστασία της εμπιστευτικότητας και ακεραιότητας των δεδομένων δοκιμών.

11.4 Γενικός Κανονισμός για την Προστασία Δεδομένων της ΕΕ (ΓΚΠΔ)

11.4.1 Άρθρο 5(1)(c) – Προβλέπει ελαχιστοποίηση δεδομένων, συμπεριλαμβανομένης της χρήσης μόνο των αναγκαίων δεδομένων για δοκιμές.

11.4.2 Άρθρο 25 – Απαιτεί προστασία δεδομένων ήδη από τον σχεδιασμό, συμπεριλαμβανομένων ελέγχων για τα περιβάλλοντα δοκιμών.

11.4.3 Άρθρο 32 – Επιβάλλει ασφαλή επεξεργασία δεδομένων προσωπικού χαρακτήρα σε όλα τα συστήματα, συμπεριλαμβανομένων των περιβαλλόντων μη παραγωγικής λειτουργίας.

11.5 Οδηγία NIS2 της ΕΕ (2022/2555)

11.5.1 Άρθρο 21(2)(e, h) – Απαιτεί ασφαλή ανάπτυξη και δοκιμές συστημάτων, ιδίως όπου οι ψηφιακές υπηρεσίες είναι εκτεθειμένες σε κυβερνοκίνδυνο.

11.6 Κανονισμός DORA της ΕΕ (2022/2554)

11.6.1 Άρθρο 9 – Τονίζει τη σημασία της ψηφιακής επιχειρησιακής ανθεκτικότητας, συμπεριλαμβανομένων των ασφαλών δοκιμών συστημάτων ΤΠΕ από ΜΜΕ στον χρηματοοικονομικό τομέα.

11.7 COBIT 2019

11.7.1 BAI07 – Διαχείριση αποδοχής αλλαγών και μετάβασης: Περιλαμβάνει ελέγχους δοκιμών για την επικύρωση νέων συστημάτων και του χειρισμού δεδομένων.

11.7.2 DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Επιβάλλει πρακτικές δοκιμών και ανάπτυξης που αποτρέπουν την κακή χρήση ή την έκθεση επιχειρησιακών δεδομένων.