					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: P29					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**

Ευθυγράμμιση με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο/Κανονισμός	**Ρήτρα/Άρθρο**	**Σχόλιο**
ISO/IEC 27001:2022	Ρήτρα 8	Σχετίζεται με τον ασφαλή σχεδιασμό και τον έλεγχο των δεδομένων δοκιμών και των περιβαλλόντων δοκιμών
ISO/IEC 27002:2022	Έλεγχοι 8.28–8.29	Καλύπτει την ασφαλή διαχείριση των δεδομένων δοκιμών και την προστασία των περιβαλλόντων δοκιμών
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Αντιμετωπίζει τις δοκιμές και την αξιολόγηση από προγραμματιστές, την προστασία δεδομένων σε αποθήκευση και την ακεραιότητα πληροφοριών
ΓΚΠΔ της ΕΕ	Άρθρα 5, 25, 32	Καλύπτει την ελαχιστοποίηση δεδομένων, την προστασία δεδομένων ήδη από τον σχεδιασμό και την ασφάλεια της επεξεργασίας στο πλαίσιο δοκιμών
Οδηγία NIS2 της ΕΕ	Άρθρο 21(2)(e), (h)	Σχετίζεται με πρακτικές ασφαλούς ανάπτυξης και δοκιμών
Κανονισμός DORA της ΕΕ	Άρθρο 9	Αφορά τα συστήματα και πρωτόκολλα ΤΠΕ και την ασφάλεια των δεδομένων δοκιμών
COBIT 2019	DSS05, BAI07	Αφορά τη διαχείριση υπηρεσιών ασφάλειας και τη διαχείριση αποδοχής αλλαγών και μετάβασης

1. Σκοπός

1.1. Η παρούσα πολιτική καθορίζει τις υποχρεωτικές απαιτήσεις για τη διαχείριση των περιβαλλόντων δοκιμών και των δεδομένων δοκιμών, ώστε να διασφαλίζονται η ασφάλεια, η εμπιστευτικότητα και η λειτουργική ακεραιότητα σε όλο τον κύκλο ζωής της ανάπτυξης λογισμικού και των δοκιμών.

1.2. Σκοπός της είναι να αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση, τη διαρροή δεδομένων και τη μόλυνση των συστημάτων παραγωγής λόγω εσφαλμένης διαχείρισης των περιβαλλόντων δοκιμών ή χρήσης πραγματικών δεδομένων σε δοκιμές.

1.3. Η πολιτική επιβάλλει τον ασφαλή χειρισμό των δεδομένων που χρησιμοποιούνται για δοκιμές, τη σκλήρυνση της υποδομής δοκιμών και την εφαρμογή ελέγχων πρόσβασης βάσει ρόλων, σε ευθυγράμμιση με τις εφαρμοστέες κανονιστικές και συμβατικές υποχρεώσεις.

2. Πεδίο εφαρμογής

2.1. Η παρούσα πολιτική εφαρμόζεται σε όλα τα περιβάλλοντα δοκιμών, δεδομένα, εργαλεία και διαδικασίες που χρησιμοποιούνται για δοκιμές λογισμικού, συστημάτων, εφαρμογών και υποδομών σε όλο τον οργανισμό.

2.2. Καλύπτει:

2.2.1. Περιβάλλοντα δοκιμών που παρέχονται εντός των εγκαταστάσεων, σε περιβάλλον νέφους ή μέσω πλατφορμών τρίτων μερών

2.2.2. Δεδομένα δοκιμών που χρησιμοποιούνται σε λειτουργικές δοκιμές, δοκιμές επιδόσεων, δοκιμές παλινδρόμησης και δοκιμές ασφάλειας

2.2.3. Χειροκίνητες δοκιμές, δοκιμές μέσω σεναρίων ενεργειών ή αυτοματοποιημένες δοκιμές (π.χ. αγωγοί CI/CD)

2.2.4. Όλο το προσωπικό που συμμετέχει στις δοκιμές, συμπεριλαμβανομένων εσωτερικών ομάδων, προμηθευτών, λοιπών τρίτων μερών και αναδόχων

2.3. Η πολιτική εφαρμόζεται ανεξαρτήτως της κρισιμότητας του συστήματος, του τύπου της εφαρμογής ή του αν η ανάπτυξη πραγματοποιείται εσωτερικά ή μέσω εξωτερικής ανάθεσης.

3. Στόχοι

3.1. Να αποτρέπεται η χρήση ενεργών, ευαίσθητων ή κανονιστικά ρυθμιζόμενων δεδομένων (π.χ. προσωπικά αναγνωρίσιμες πληροφορίες (PII), δεδομένα κατόχων καρτών) σε περιβάλλοντα δοκιμών, εκτός εάν έχουν ανωνυμοποιηθεί ή έχουν εγκριθεί ειδικά.

3.2. Να διασφαλίζεται πλήρης διαχωρισμός δικτύου και πρόσβασης μεταξύ των περιβαλλόντων δοκιμών και του περιβάλλοντος παραγωγής, ώστε να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή η μόλυνση συστημάτων.

3.3. Να απαιτείται κρυπτογράφηση, απόκρυψη δεδομένων ή δημιουργία συνθετικών δεδομένων όταν απαιτούνται αντιπροσωπευτικά δεδομένα για σκοπούς δοκιμών.

3.4. Να μειώνεται η πιθανότητα αστοχιών συμμόρφωσης, έκθεσης δεδομένων πελατών ή λειτουργικής διαταραχής που απορρέει από μη ασφαλή δεδομένα δοκιμών ή περιβάλλοντα δοκιμών.

3.5. Να ευθυγραμμίζεται ο χειρισμός δεδομένων δοκιμών με πρότυπα του κλάδου (ISO, NIST, COBIT) και κανονιστικές απαιτήσεις όπως ο ΓΚΠΔ της ΕΕ, η Οδηγία NIS2 της ΕΕ και ο Κανονισμός DORA της ΕΕ.

4. Ρόλοι και αρμοδιότητες

4.1. Επικεφαλής Ασφάλειας Πληροφοριών (CISO)

4.1.1. Έχει την κυριότητα της παρούσας πολιτικής και διασφαλίζει την εφαρμογή τεχνικών και οργανωτικών μέτρων για τα δεδομένα δοκιμών και τα περιβάλλοντα δοκιμών.

4.1.2. Εγκρίνει τη χρήση πραγματικών ή ευαίσθητων δεδομένων σε δοκιμές με κατάλληλη αιτιολόγηση και αντισταθμιστικές δικλίδες.

4.2. Επικεφαλής Διασφάλισης Ποιότητας/Δοκιμών

4.2.1. Συντονίζει τον σχεδιασμό δοκιμών και διασφαλίζει ότι όλες οι δραστηριότητες δοκιμών συμμορφώνονται με τις απαιτήσεις της παρούσας πολιτικής.

4.2.2. Επικυρώνει τον κατάλληλο διαχωρισμό, την πρόσβαση και την προετοιμασία δεδομένων για κάθε φάση δοκιμών.

[... 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 και να επικαιροποιείται όπου απαιτείται, ώστε να αντικατοπτρίζει:

9.1.1. Αλλαγές στις κανονιστικές απαιτήσεις (π.χ. ΓΚΠΔ της ΕΕ, Κανονισμός DORA της ΕΕ, Οδηγία NIS2 της ΕΕ)

9.1.2. Την υιοθέτηση νέων εργαλείων δοκιμών, πλατφορμών ή αγωγών αυτοματοποίησης

9.1.3. Ευρήματα εσωτερικού ελέγχου ή συστάσεις μετά από περιστατικά

9.1.4. Επέκταση διαδικασιών ανάπτυξης ή διασφάλισης ποιότητας που μεταβάλλουν τον χειρισμό δεδομένων δοκιμών ή τη χρήση περιβαλλόντων

9.2. Ο CISO έχει την ευθύνη να εκκινεί την ανασκόπηση σε συνεργασία με:

9.2.1. Επικεφαλής Διασφάλισης Ποιότητας/Δοκιμών

9.2.2. Διευθυντές DevOps και Υποδομών

9.2.3. Ομάδες Ανάπτυξης Εφαρμογών

9.2.4. Υπεύθυνο Προστασίας Δεδομένων (DPO) και Νομικό Σύμβουλο

9.3. Όλες οι αναθεωρήσεις πρέπει:

9.3.1. Να ελέγχονται ως προς την έκδοση και να αποθηκεύονται στο κεντρικό Αποθετήριο Εγγράφων

9.3.2. Να κοινοποιούνται στο επηρεαζόμενο προσωπικό μέσω επίσημων διαύλων (π.χ. ειδοποιήσεις ISMS, ενημερώσεις ομάδων)

9.3.3. Να συνδέονται με επικαιροποιήσεις στα συναφή τεχνικά πρότυπα, στους ελέγχους και στις λειτουργικές διαδικασίες

9.4. Ενδιάμεσες ανασκοπήσεις βάσει εναυσμάτων πρέπει να διενεργούνται αμέσως μετά από οποιοδήποτε από τα ακόλουθα:

9.4.1. Διαρροή δεδομένων ή παραβίαση που αφορά περιβάλλοντα δοκιμών

9.4.2. Μη συμμόρφωση σε έλεγχο σχετική με τον χειρισμό δεδομένων δοκιμών

9.4.3. Σημαντικές αλλαγές σε νομικές υποχρεώσεις ή στην αρχιτεκτονική ΤΠ

10. Συναφείς πολιτικές και διασυνδέσεις

10.1. Η παρούσα πολιτική είναι στενά διασυνδεδεμένη με τις ακόλουθες πολιτικές, ώστε να διασφαλίζεται ο ασφαλής και σύμφωνος χειρισμός των δεδομένων δοκιμών και των περιβαλλόντων δοκιμών:

10.1.1. P1 – Πολιτική Ασφάλειας Πληροφοριών: Θεσπίζει τις γενικές αρχές ασφάλειας που διέπουν την προστασία των δεδομένων δοκιμών και τη διαχείριση των περιβαλλόντων.

10.1.2. P5 – Πολιτική Διαχείρισης Αλλαγών: Εφαρμόζεται στη δημιουργία, επικαιροποίηση και απόσυρση των περιβαλλόντων δοκιμών και των αγωγών εγκατάστασης.

10.1.3. P13 – Πολιτική Ταξινόμησης και Επισήμανσης Δεδομένων: Καθοδηγεί την επιλογή δεδομένων δοκιμών και την εφαρμογή ελέγχων βάσει ευαισθησίας.

10.1.4. P14 – Πολιτική Διατήρησης και Διάθεσης Δεδομένων: Καθορίζει χρονοδιαγράμματα διατήρησης και απαιτήσεις ασφαλούς διάθεσης για τα σύνολα δεδομένων δοκιμών.

10.1.5. P15 – Πολιτική Αντιγράφων Ασφαλείας και Αποκατάστασης: Επιβάλλει πρακτικές αντιγράφων ασφαλείας και επικύρωση ανάκαμψης για τα περιβάλλοντα δοκιμών.

10.1.6. P18 – Πολιτική Κρυπτογραφικών Ελέγχων: Προσδιορίζει τα υποχρεωτικά πρότυπα κρυπτογράφησης για δεδομένα σε αποθήκευση και σε μεταφορά εντός πλατφορμών δοκιμών.

10.1.7. P22 – Πολιτική Καταγραφής και Παρακολούθησης: Διέπει την ορατότητα και την ανίχνευση ανωμαλιών για τις δραστηριότητες των περιβαλλόντων δοκιμών.

10.1.8. P30 – Πολιτική Αντιμετώπισης Περιστατικών: Καθορίζει την κλιμάκωση και την αποκατάσταση για παραβιάσεις ή περιστατικά που αφορούν συστήματα δοκιμών.

10.1.9. P33 – Πολιτική Παρακολούθησης Ελέγχων και Συμμόρφωσης: Επιτρέπει την επικύρωση της τήρησης της πολιτικής και τη συνεχή διασφάλιση.

11. Πρότυπα και πλαίσια αναφοράς

11.1. Η παρούσα πολιτική ευθυγραμμίζεται με διεθνή πρότυπα κυβερνοασφάλειας και κανονιστικά πλαίσια που επιβάλλουν τον ασφαλή χειρισμό δεδομένων δοκιμών και την προστασία περιβαλλόντων μη παραγωγικής λειτουργίας.

11.2. ISO/IEC 27001:

11.2.1. Ρήτρα 8.1 - Επιβάλλει τον ασφαλή σχεδιασμό και έλεγχο των δεδομένων δοκιμών και των περιβαλλόντων δοκιμών.

11.3. ISO/IEC 27002:2022 – Έλεγχοι 8.28–8.29:

11.3.1. Παράρτημα Α, Έλεγχος 8.28 – Ασφαλή δεδομένα δοκιμών: Απαιτεί την προστασία των δεδομένων δοκιμών που χρησιμοποιούνται στις φάσεις ανάπτυξης και δοκιμών μέσω ανωνυμοποίησης, απόκρυψης δεδομένων ή δημιουργίας συνθετικών δεδομένων.

11.3.2. Παράρτημα Α, Έλεγχος 8.29 – Προστασία περιβαλλόντων δοκιμών: Απαιτεί διαχωρισμό από την παραγωγή, ελέγχους πρόσβασης και σκλήρυνση περιβάλλοντος για τα συστήματα δοκιμών.

11.3.3. Οι έλεγχοι αυτοί περιγράφουν απαιτήσεις για την ασφαλή διαχείριση των δεδομένων που χρησιμοποιούνται κατά τις δοκιμές και για την προστασία συστημάτων μη παραγωγικής λειτουργίας από κακή χρήση, παραβίαση της ασφάλειας ή μόλυνση.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Δοκιμές και αξιολόγηση από προγραμματιστές: Καθορίζει προσδοκίες για ασφαλείς, επαναλήψιμες διαδικασίες δοκιμών με κατάλληλους ελέγχους δεδομένων.

11.4.2. SC-28 – Προστασία πληροφοριών σε αποθήκευση: Ευθυγραμμίζεται με την κρυπτογράφηση δεδομένων δοκιμών που αποθηκεύονται σε συστήματα μη παραγωγικής λειτουργίας.

11.4.3. SC-32 – Ακεραιότητα πληροφοριών: Υποστηρίζει την επικύρωση δεδομένων, την πρόληψη αλλοίωσης και τους ελέγχους εισόδου/εξόδου κατά τις δοκιμές.

11.5. ΓΚΠΔ της ΕΕ (2016/679):

11.5.1. Άρθρο 5 – Ελαχιστοποίηση δεδομένων: Απαγορεύει τη μη αναγκαία χρήση δεδομένων προσωπικού χαρακτήρα σε δοκιμές.

11.5.2. Άρθρο 25 – Προστασία δεδομένων ήδη από τον σχεδιασμό και εξ ορισμού: Απαιτεί την εφαρμογή τεχνικών προστασίας δεδομένων από την έναρξη του κύκλου ανάπτυξης και δοκιμών.

11.5.3. Άρθρο 32 – Ασφάλεια της επεξεργασίας: Επιβάλλει δικλίδες ασφαλείας για περιβάλλοντα δοκιμών που χειρίζονται δεδομένα προσωπικού χαρακτήρα ή ευαίσθητα δεδομένα.

11.6. Οδηγία NIS2 της ΕΕ (2022/2555):

11.6.1. Άρθρο 21(2)(e, h): Απαιτεί ασφαλείς διαδικασίες ανάπτυξης λογισμικού και δοκιμών, με έμφαση στην προστασία από μη εξουσιοδοτημένη πρόσβαση και διαρροή δεδομένων.

11.7. Κανονισμός DORA της ΕΕ (2022/2554):

11.7.1. Άρθρο 9 – Συστήματα και πρωτόκολλα ΤΠΕ: Απαιτεί οι διαδικασίες δοκιμών να υποστηρίζουν την ανθεκτικότητα και να προστατεύουν τα λειτουργικά δεδομένα από παραβίαση της ασφάλειας ή μη εξουσιοδοτημένη γνωστοποίηση.

11.8. COBIT 2019:

11.8.1. DSS05 – Διαχείριση υπηρεσιών ασφάλειας: Υποστηρίζει την εφαρμογή πολιτικών ασφάλειας σε όλα τα περιβάλλοντα, συμπεριλαμβανομένων των περιβαλλόντων μη παραγωγικής λειτουργίας.

11.8.2. BAI07 – Διαχείριση αποδοχής αλλαγών και μετάβασης: Καλύπτει την επίσημη διαδικασία μετάβασης από τις δοκιμές στην παραγωγή, συμπεριλαμβανομένων των ελέγχων δεδομένων και περιβάλλοντος.