

Digital investigation briefing

Decide what to preserve, what can be established and which deliverables to request.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ Name the authorised owner, question and reporting recipients.

☐ List relevant systems, accounts, dates and source owners.

☐ Identify expiring records and agree preservation priorities.

☐ Record collection parameters, time zones and integrity checks.

☐ Require facts, inferences and unresolved questions to be separated.

☐ Agree a review checkpoint, scope changes and evidence handling after closure.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: NIST SP 800-86

Προετοιμασία ψηφιακής έρευνας

Αποφασίστε τι διατηρείται, τι μπορεί να τεκμηριωθεί και ποια παραδοτέα χρειάζεστε.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Ορίστε εξουσιοδοτημένο υπεύθυνο, ερώτημα και αποδέκτες.

☐ Καταγράψτε συστήματα, λογαριασμούς, ημερομηνίες και υπευθύνους πηγών.

☐ Εντοπίστε αρχεία που λήγουν και συμφωνήστε προτεραιότητες διατήρησης.

☐ Καταγράψτε παραμέτρους συλλογής, ζώνες ώρας και ελέγχους ακεραιότητας.

☐ Ζητήστε διαχωρισμό γεγονότων, ερμηνειών και ανοικτών ερωτημάτων.

☐ Συμφωνήστε σημείο αξιολόγησης, αλλαγές αντικειμένου και τελικό χειρισμό τεκμηρίων.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: NIST SP 800-86

AI-agent release assessment

Decide whether a specific release may operate, under which permissions and with which restrictions.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ List the task, users, approved data and prohibited actions.

☐ Record model, tool, policy and connector versions.

☐ Test cross-user retrieval and untrusted document instructions.

☐ Bind approvals to exact destinations, parameters and expiry.

☐ Test timeouts, retries, cancellation and partial completion.

☐ Name the release approver and rehearse the stop and recovery procedure.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: OWASP — Excessive agency · OWASP — Prompt injection

Αξιολόγηση παραγωγικής χρήσης AI agent

Αποφασίστε αν μια συγκεκριμένη έκδοση μπορεί να λειτουργήσει, με ποια δικαιώματα και περιορισμούς.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Καταγράψτε εργασία, χρήστες, εγκεκριμένα δεδομένα και απαγορευμένες ενέργειες.

☐ Καταγράψτε εκδόσεις μοντέλου, εργαλείων, πολιτικών και συνδέσμων.

☐ Ελέγξτε πρόσβαση άλλου χρήστη και μη έμπιστες οδηγίες εγγράφων.

☐ Συνδέστε εγκρίσεις με ακριβή προορισμό, παραμέτρους και λήξη.

☐ Δοκιμάστε καθυστερήσεις, επαναλήψεις, ακύρωση και μερική ολοκλήρωση.

☐ Ορίστε υπεύθυνο έγκρισης και δοκιμάστε διακοπή και ανάκαμψη.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: OWASP — Υπερβολική αυτονομία · OWASP — Prompt injection

GDPR consulting scope

Define a comparable scope, realistic dependencies and verifiable deliverables before asking for a price.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ List entities, locations, processing activities and critical systems.

☐ Describe current documentation and the evidence available.

☐ Separate assessment, implementation and ongoing support.

☐ Identify internal owners and required legal or engineering input.

☐ Request deliverables, exclusions and acceptance criteria in writing.

☐ Agree change control, review rounds, handover and recurring tasks.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: EDPB — Data protection guide for small business

Αντικείμενο συμβουλευτικής GDPR

Ορίστε συγκρίσιμο αντικείμενο, ρεαλιστικές εξαρτήσεις και ελέγξιμα παραδοτέα πριν ζητήσετε τιμή.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Καταγράψτε οντότητες, εγκαταστάσεις, επεξεργασίες και κρίσιμα συστήματα.

☐ Περιγράψτε την υπάρχουσα τεκμηρίωση και τα διαθέσιμα στοιχεία.

☐ Διαχωρίστε αξιολόγηση, υλοποίηση και συνεχή υποστήριξη.

☐ Ορίστε εσωτερικούς υπευθύνους και αναγκαία νομική ή τεχνική συμμετοχή.

☐ Ζητήστε γραπτά παραδοτέα, εξαιρέσεις και κριτήρια αποδοχής.

☐ Συμφωνήστε διαχείριση αλλαγών, ελέγχους, παράδοση και επαναλαμβανόμενες εργασίες.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: ΕΣΠΔ — Οδηγός προστασίας δεδομένων για μικρές επιχειρήσεις

Acquisition cyber due diligence

Identify which security uncertainties affect the transaction and which actions belong in integration.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ Identify the investment thesis, transaction boundary and decision date.

☐ List critical assets, services, entities and seller dependencies.

☐ Request dated evidence for privileged access, recovery and incident handling.

☐ Record permitted tests, exclusions and unanswered questions.

☐ Separate pre-completion decisions from the integration backlog.

☐ Assign owners and verification criteria to Day 1 controls and remediation.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: NIST Cybersecurity Framework · NIST SP 800-161 Rev. 1

Έλεγχος κυβερνοασφάλειας πριν από εξαγορά

Εντοπίστε ποιες αβεβαιότητες ασφάλειας επηρεάζουν τη συναλλαγή και ποιες ενέργειες αφορούν την ενσωμάτωση.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Ορίστε επενδυτική λογική, όρια συναλλαγής και ημερομηνία απόφασης.

☐ Καταγράψτε κρίσιμα στοιχεία, υπηρεσίες, οντότητες και εξαρτήσεις από τον πωλητή.

☐ Ζητήστε χρονολογημένα στοιχεία πρόσβασης, ανάκτησης και χειρισμού περιστατικών.

☐ Καταγράψτε επιτρεπόμενες δοκιμές, εξαιρέσεις και ανοικτά ερωτήματα.

☐ Διαχωρίστε αποφάσεις πριν την ολοκλήρωση από το πλάνο ενσωμάτωσης.

☐ Ορίστε υπευθύνους και επαλήθευση μέτρων πρώτης ημέρας και διορθώσεων.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: NIST Cybersecurity Framework · NIST SP 800-161 Rev. 1

Employee-departure investigation

Determine what the evidence supports while preserving material and controlling continuing exposure.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ Appoint a case owner and agree HR, legal and privacy coordination.

☐ Write the question, affected information and relevant period.

☐ Coordinate containment and preservation before routine deletion or reassignment.

☐ Map actual audit coverage, retention and collection permissions.

☐ Test legitimate explanations and separate account activity from attribution.

☐ Agree report recipients, next checkpoint and final retention or disposal instructions.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: NIST SP 800-86 · Microsoft — Audit log activities

Διερεύνηση κατά την αποχώρηση στελέχους

Προσδιορίστε τι στηρίζουν τα στοιχεία, διατηρώντας το υλικό και περιορίζοντας συνεχιζόμενη έκθεση.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Ορίστε υπεύθυνο και συντονισμό με HR, νομικούς και προστασία δεδομένων.

☐ Διατυπώστε ερώτημα, επηρεαζόμενες πληροφορίες και περίοδο.

☐ Συντονίστε περιορισμό και διατήρηση πριν από διαγραφή ή αλλαγή χρήστη.

☐ Χαρτογραφήστε πραγματική καταγραφή, διατήρηση και δικαιώματα συλλογής.

☐ Ελέγξτε νόμιμες εξηγήσεις και διαχωρίστε λογαριασμό από απόδοση ενεργειών.

☐ Συμφωνήστε αποδέκτες, επόμενο σημείο ελέγχου και τελική διατήρηση ή διάθεση.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: NIST SP 800-86 · Microsoft — Συμβάντα αρχείων ελέγχου

Enterprise RAG access review

Approve a RAG release only when retrieval, citations, cache and history follow an explicit access policy.

Case / project: _____ Owner: _____

Date: _____ Version / scope: _____

Record status, owner and a safe evidence reference. Do not enter credentials or real personal data here.

☐ Map source documents, chunks, metadata, citations, cache and history.

☐ Resolve users and tenants from trusted authentication, not chat inputs.

☐ Define permission propagation and the required revocation interval.

☐ Test exact queries, paraphrases, direct links and warm-cache responses.

☐ Use synthetic markers with both authorised and denied users.

☐ Record release versions, failures, restrictions and re-test triggers.

Open questions / next decision

Read the full guide at trust-it.gr

Sources: OWASP — Vector and embedding weaknesses · Microsoft — Document-level access control

Έλεγχος πρόσβασης εταιρικού RAG

Εγκρίνετε έκδοση RAG όταν ανάκτηση, παραπομπές, cache και ιστορικό ακολουθούν ρητή πολιτική πρόσβασης.

Υπόθεση / έργο: _____ Υπεύθυνος: _____

Ημερομηνία: _____ Έκδοση / πεδίο: _____

Σημειώστε κατάσταση, υπεύθυνο και ασφαλή αναφορά στοιχείων. Μην καταγράφετε κωδικούς ή πραγματικά προσωπικά δεδομένα εδώ.

☐ Χαρτογραφήστε έγγραφα, αποσπάσματα, μεταδεδομένα, παραπομπές, cache και ιστορικό.

☐ Προσδιορίστε χρήστες και οργανισμούς από έμπιστη αυθεντικοποίηση.

☐ Ορίστε ενημέρωση δικαιωμάτων και απαιτούμενο διάστημα ανάκλησης.

☐ Δοκιμάστε ακριβή ερωτήματα, παραφράσεις, συνδέσμους και έτοιμες απαντήσεις cache.

☐ Χρησιμοποιήστε συνθετικούς δείκτες με εξουσιοδοτημένους και μη χρήστες.

☐ Καταγράψτε εκδόσεις, αστοχίες, περιορισμούς και αφορμές επανελέγχου.

Ανοικτά ερωτήματα / επόμενη απόφαση

Διαβάστε τον πλήρη οδηγό στο trust-it.gr

Πηγές: OWASP — Αδυναμίες διανυσμάτων και embeddings · Microsoft — Πρόσβαση σε επίπεδο εγγράφου