Procedure de Gestion des Incidents Informatiques

Guide operationnel - Support IT - ITSM

Objectif
Assurer une prise en charge rapide, structuree et traçable des incidents afin de proteger la continuite des activites.

Perimetre
Postes, reseau, applications, acces, securite, services cloud et telephonie.

Proprietaire	Version	Application	Revision
Responsable IT	V1.0	Immediate	Annuelle

1. Cadre et definitions

Un incident informatique est tout evenement non planifie qui degrade (ou risque de degrader) un service du systeme d'information. Cette procedure standardise la declaration, la priorisation, la resolution et la cloture des incidents.

Objectifs

- Diminuer les interruptions de service et l'impact metier.
- Assurer une communication claire (utilisateur, support, responsables).
- Garantir la traçabilite via un ticket unique.
- Capitaliser les causes frequentes et prevenir la recurrence.

2. Typologie et criticite

Categorie	Exemples	Couverture
Materiel	PC en panne, imprimante HS, batterie, ecran	Support / Parc
Logiciel	Application bloque, erreur, mise a jour	Support / Editeur
Reseau	Wi-Fi instable, coupure, DNS, VPN	Reseau / Telecom
Securite	Phishing, malware, compte compromis	SecOps / IT

Matrice de priorite (Impact x Urgence)

	Urgence Faible	Urgence Moyenne	Urgence Haute
Impact Faible	P4	P3	P3
Impact Moyen	P3	P2	P2
Impact Eleve	P2	P1	P1

Engagements de service (SLA) - Exemple

Priorite	Cible prise en charge	Cible resolution	Exemple
P1	15 min	4 h	Service critique indisponible (metier stop)
P2	1 h	8 h	Degradation majeure (grand nombre d'utilisateurs)
P3	4 h	48 h	Incident standard (contournement possible)
P4	1 j	5 j	Demande a faible impact / question

3. Processus operatoire

Le processus ci-dessous s'applique a tout incident : detection, ticket, qualification, resolution, cloture, puis capitalisation. Un seul ticket par incident (reference unique) est obligatoire.

3.1 Regles de declaration (utilisateur)

Ce que l'utilisateur doit fournir dans le ticket

- Service / application impacte(e) + localisation (site, etage, bureau).
- Symptome observe + message d'erreur (copie / capture si possible).
- Depuis quand ? (heure approx.) + actions faites juste avant (MAJ, branchement, etc.).
- Nombre de personnes impactees (seul / equipe / site).
- Criticite metier (activite arretee ? contournement possible ?).

3.2 Escalade et gestion de crise

Quand escalader immediatement

- Priorite P1 ou suspicion securite (phishing, malware, compte compromis).
- Incident recurrent sans solution durable (3 occurrences sur 30 jours).
- Incident multi-sites ou impactant un service critique (ERP, reseau, messagerie).

Communication standardisee

Etape	Canal	Message attendu
Accuse de reception	Outil ticket / email	Numero ticket + priorite + delai estime
Mise a jour	Ticket + Teams/Slack si P1-P2	Etat d'avancement + actions en cours
Resolution	Ticket	Solution + consignes utilisateur
Incident securite	Procedure SecOps	Isolement + consignes + rapport

4. Roles, responsabilites et pilotage

RACI (R=Realise, A=Approuve, C=Consulte)

Activite	Utilisateur	Support N1	Support N2/N3	Resp. IT	SecOps
Declaration ticket	R	A		C	
Qualification / priorite	C	R	C	A	C
Resolution standard	C	R	C	A	
Incident majeur (P1)	C	R	R	A	C
Incident securite	C	C	R	A	R
Cloture / validation	R	A	C	C	C
Post-mortem / capitalisation	C	R	R	A	C

Indicateurs de performance (KPI) - tableau de bord

MTTR Temps moyen de resolution	**Cible** P1: 4h P2: 8h	**Taux de respect SLA** Tickets resolus dans le delai	**Suivi** Hebdo / Mensuel
Satisfaction utilisateurs Note post-cloture	**Objectif** >= 4/5	**Top causes** Categories recurrentes	**Action** Prevention + KB

Annexe - Fiche ticket (modele a recopier dans l'outil de support)

Champ	Contenu a saisir
Demandeur	Nom, service, contact
Service impacte	Application / reseau / poste / acces
Description	Symptomes, message d'erreur, contexte
Impact	Nombre d'utilisateurs, activite arretee ?
Urgence	Delai metier, echeance
Priorite proposee	P1 / P2 / P3 / P4
Pieces jointes	Capture, logs, photo
Validation cloture	OK utilisateur + commentaire