

INCIDENT RESPONSE PLAN

SAMPLE DENTAL GROUP (MADE UP)

What to do, who to call, and who decides when something goes wrong.

Version 2.0 · Plan owner: Morgan Sample, Office Manager · Approved by Dr. R. Example, Owner on Oct 14, 2026 · Next review: Oct 14, 2027

Prepared with Example Security Partners · Confidential

THE FIRST HOUR

Print this page and keep it where people can find it without a computer.

- 1 Stop and report. Tell Morgan Sample, the incident lead, right away. Reporting quickly is never punished.
- 2 Disconnect, do not power off. Unplug the network cable or turn off Wi-Fi on the affected machine. Leave it on so evidence is kept.
- 3 Do not try to fix it, delete things, or contact the attacker.
- 4 Write down what you saw, when, and what you did. Take a photo of the screen with your phone.
- 5 The incident lead declares a level, opens the incident log, and calls the people listed below.
- 6 For Level 2 or 3: call the cyber insurance hotline before hiring anyone.
- 7 If email or chat may be affected, switch to: Group text on personal phones, then the conference bridge (555) 010-0190.

CALL FIRST

Role	Person or role	Phone	Backup	Backup's phone
Incident lead	Morgan Sample	(555) 010-0143	Alex Sample, Example Security Partners	(555) 010-0199
Executive decision-maker	Dr. R. Example	(555) 010-0142	Dr. T. Sample, associate dentist	(555) 010-0144
Technical lead	Example IT Services on-call	(555) 010-0150	Alex Sample, Example Security Partners	(555) 010-0199
Communications lead	Jamie Example	(555) 010-0145	Morgan Sample	(555) 010-0143
Finance lead	Robin Sample	(555) 010-0146	Dr. R. Example	(555) 010-0142
Legal counsel	Sample & Example LLP	(555) 010-0172	Insurer's breach coach	(555) 010-0170

Outside help	Company, person or role	Phone
Cyber insurance hotline	Sample Mutual Insurance, breach line	(555) 010-0170
Breach counsel (lawyer)	Sample & Example LLP	(555) 010-0172
Bank fraud line	Sample Community Bank, fraud desk	(555) 010-0176

HOW THIS PLAN WORKS

This plan tells Sample Dental Group (made up) how to respond to a cybersecurity incident: an event that harms, or could harm, its systems, data or ability to operate. It is written to be used under pressure by people who are not security specialists.

SEVERITY LEVELS

Level	What it means and who acts
Level 1: Minor	One PC, phone or mailbox, no patient records involved, and already contained. Example IT Services handles it and tells the office manager the same day.
Level 2: Serious	Several PCs or accounts, possible access to patient records, or the schedule, imaging or phones down for part of a day. The office manager gathers the team within one hour, tells Dr. Example, and notifies the insurer.
Level 3: Critical	The practice cannot see patients, ransomware, confirmed theft of patient records, or money lost to fraud. The whole team meets now and Dr. Example leads decisions. The insurer and breach counsel are called immediately.

THE FIVE PHASES

- 1 Identify: confirm something is wrong, declare a level, start the log.
- 2 Contain: cut affected systems and accounts off so the damage stops spreading.
- 3 Remove: find how the attacker got in and close it; remove what they left behind.
- 4 Recover: restore systems in the agreed order from clean backups, and watch for a return.
- 5 Learn: hold an after-action review within two weeks and update this plan.

ROLES

Role	Person or role	What they do
Incident lead	Morgan Sample	Runs the response, declares the level, keeps the log.
Executive decision-maker	Dr. R. Example	Owner or senior leader. Approves spending, shutdowns and outside statements.
Technical lead	Example IT Services on-call	Isolates systems, preserves evidence, restores service. Often the IT provider.
Communications lead	Jamie Example	Tells staff, customers and the press, using approved wording.
Finance lead	Robin Sample	Calls the bank, stops payments, tracks costs for the insurance claim.
Legal counsel	Sample & Example LLP	Advises on notification duties and protects the investigation. Usually outside counsel.

WHO TO CALL

RESPONSE TEAM

Role	Person or role	Phone	Email	Backup	Backup's phone
Incident lead	Morgan Sample	(555) 010-0143	morgan@example.com	Alex Sample, Example Security Partners	(555) 010-0199
Executive decision-maker	Dr. R. Example	(555) 010-0142	dr.example@example.com	Dr. T. Sample, associate dentist	(555) 010-0144
Technical lead	Example IT Services on-call	(555) 010-0150	help@example.com	Alex Sample, Example Security Partners	(555) 010-0199
Communications lead	Jamie Example	(555) 010-0145	jamie@example.com	Morgan Sample	(555) 010-0143
Finance lead	Robin Sample	(555) 010-0146	billing@example.com	Dr. R. Example	(555) 010-0142
Legal counsel	Sample & Example LLP	(555) 010-0172	breach@example.com	Insurer's breach coach	(555) 010-0170

OUTSIDE HELP

For	Company, person or role	Phone	Note
Cyber insurance hotline	Sample Mutual Insurance, breach line	(555) 010-0170	Call first in a Level 2 or 3 incident. Policy schedule is in the front office safe.
Breach counsel (lawyer)	Sample & Example LLP	(555) 010-0172	On the insurer's panel. Confirmed October 2026.
Incident response firm	Example Forensics (insurer panel firm)	(555) 010-0174	Engaged through the insurer, not directly.
IT provider	Example IT Services	(555) 010-0150	After-hours line answers 24/7. Quote the practice's client code.
Bank fraud line	Sample Community Bank, fraud desk	(555) 010-0176	For payment fraud. Ask for a wire or ACH recall. Minutes matter.
FBI / IC3	FBI Internet Crime Complaint Center	Online at ic3.gov	Report fraud and ransomware. The bank needs the complaint number.
CISA	Cybersecurity and Infrastructure Security Agency	report@cisa.gov	cisa.gov/report
Dental software vendor	Example Dental Software support	(555) 010-0178	Practice management and imaging. Business associate agreement on file.

Passwords, PINs and full account or policy numbers are not printed in this plan. Printed copies are kept at: Front office safe; Dr. Example's home office; Example Security Partners case file.

WHAT TO ISOLATE AND RESTORE

Systems are listed in the order they should be restored. Isolating a system means cutting it off from the network, not turning it off.

#	System	How to cut it off	Who may do it	Can be down	Backup	Restored by
1	Practice management and scheduling server	Unplug the server's network cable in the back-office rack. Leave it powered on.	Technical lead or office manager	4 hours; paper day sheets after that	Nightly to the cloud backup service; weekly copy to an offline drive	Example IT Services with Example Dental Software
2	Digital X-ray and imaging PCs (operatories 1 to 6)	Unplug the network cable at each imaging PC. Do not unplug the sensors.	Any clinical staff member	1 day; refer urgent imaging	Images sync nightly to the practice management server	Example IT Services
3	Microsoft 365 email and shared files	Block sign-in and sign out all sessions for affected accounts in the admin center.	Technical lead	1 day; use phones and group text	Cloud-to-cloud backup, 1 year kept	Example IT Services
4	Front desk PCs and card terminal	Turn off Wi-Fi and unplug the network cable. Card terminal: switch to the cellular backup.	Office manager	1 day; take card payments on the terminal's cellular mode	Standard build; no data kept locally	Example IT Services
5	Phones (cloud phone system)	Forward the main line to the office manager's cell from the provider's portal.	Office manager	2 hours	Provider-hosted	Phone provider, via Example IT Services
6	Firewall and office Wi-Fi	Unplug the internet line from the firewall to cut the whole office off.	Technical lead, or Dr. Example on IT's advice	Same day	Configuration saved by Example IT Services	Example IT Services

KEEPING EVIDENCE

- Leave affected machines powered on and disconnected until the technical lead or the response firm says otherwise.
- Do not delete suspicious emails, files or accounts. Move nothing; note where it is.
- Save logs before they roll over: sign-in, email, firewall and endpoint.
- Record every action in the incident log with the time and the person.

WHO COMMUNICATES

Audience	Who speaks (person or role)
Staff	Morgan Sample, Office Manager
Customers	Dr. R. Example, with Jamie Example
Press and social media	Dr. R. Example only
Regulators	Breach counsel (Sample & Example LLP)
Approves anything said outside the company	Dr. R. Example, after breach counsel has reviewed it

- Only the people named above speak for the company. Everyone else says: "I can't comment, but I'll put you in touch with the right person."
- Say only what is confirmed. Do not guess at causes, numbers or blame.
- Legal counsel reviews every outside statement before it goes out.
- If email or chat is down or may be watched, the team uses: Group text on personal phones, then the conference bridge (555) 010-0190.
- The team meets at: Back-office break room; if the office is closed, the conference bridge.

NOTIFICATION DUTIES TO CHECK WITH COUNSEL

- ☐ Cyber insurance policy: notice as soon as possible, and before hiring outside firms
- ☐ State breach notification laws, for residents whose personal information was exposed
- ☐ HIPAA: patients and HHS, without unreasonable delay and within 60 days
- ☐ Payment cards: the card processor or acquiring bank, immediately
- ☐ Customer contracts with a security notice clause
- ☐ Law enforcement, for fraud, extortion or theft

Business associate agreements: the dental software vendor and the billing clearinghouse must tell the practice of any breach of patient data, and the practice may owe them notice too. Dental plan contracts may require notice of a breach affecting their members.

Counsel decides which duties apply and when each clock starts.

PLAYBOOK: RANSOMWARE

How you will know: Files will not open, a ransom note appears, or many systems fail at once.

FIRST HOUR

- ☐ The technical lead (Example IT Services on-call) disconnects affected machines from the network (unplug the cable, turn off Wi-Fi). Leave them powered on.
- ☐ The technical lead (Example IT Services on-call) disables remote access and any shared administrator accounts that may be in use.
- ☐ The incident lead (Morgan Sample) declares a Level 3 incident and opens the incident log.
- ☐ The incident lead (Morgan Sample) calls the cyber insurance hotline before hiring anyone or contacting the attacker.
- ☐ The technical lead (Example IT Services on-call) checks that backups exist and are not connected to the affected network.
- ☐ The executive decision-maker (Dr. R. Example) decides which operations continue on paper or by phone.

FIRST DAY

- ☐ Work with the insurer's response firm to find how the attacker got in and what was reached.
- ☐ Legal counsel (Sample & Example LLP) advises on whether data was taken and who must be told.
- ☐ The communications lead (Jamie Example) tells staff what happened, what not to use, and where to send questions.
- ☐ Report to the FBI (ic3.gov) and CISA (cisa.gov/report).
- ☐ The executive decision-maker (Dr. R. Example) takes any ransom decision only with counsel and the insurer.

RECOVER

- ☐ Rebuild systems from clean media and restore data from backups known to be clean.
- ☐ Reset every password and sign-in session, starting with administrators.
- ☐ Restore the most important systems first, in the order in this plan.
- ☐ Watch closely for a return for at least 30 days.

DO NOT

- Do not turn machines off or wipe them before evidence is taken.
- Do not contact the attacker or pay without counsel and the insurer.
- Do not restore backups onto a network that is still compromised.

PLAYBOOK: PAYMENT FRAUD BY EMAIL

How you will know: A payment went to the wrong account, or someone asks to change bank details or send an urgent wire.

FIRST HOUR

- ☐ The finance lead (Robin Sample) calls the bank's fraud line and asks for a recall of the payment. Minutes matter.
- ☐ The incident lead (Morgan Sample) declares a Level 2 or 3 incident and opens the incident log.
- ☐ The technical lead (Example IT Services on-call) resets the password and signs out all sessions for any mailbox involved, and removes forwarding or inbox rules.
- ☐ The finance lead (Robin Sample) stops all pending payments to the changed account.
- ☐ Report to the FBI at ic3.gov with the transaction details. This starts the bank recovery process.

FIRST DAY

- ☐ The technical lead (Example IT Services on-call) reviews sign-in and mailbox rule history to see how long the attacker had access.
- ☐ The incident lead (Morgan Sample) calls the insurer; many policies cover funds transfer fraud only with prompt notice.
- ☐ The finance lead (Robin Sample) checks every payment detail change made in the last 90 days.
- ☐ The communications lead (Jamie Example) warns customers or vendors who may have received fake messages.

RECOVER

- ☐ Require a call-back to a known number for every new or changed payment detail.
- ☐ Require two approvers above a set amount.
- ☐ Turn on multi-factor authentication for every mailbox.

DO NOT

- Do not wait to see if the payment bounces. Call the bank now.
- Do not delete the fraudulent emails; they are evidence.
- Do not use contact details from the suspicious message to verify it.

PLAYBOOK: COMPROMISED ACCOUNT

How you will know: Sign-in alerts from unknown places, messages sent that the person did not write, or a password that stops working.

FIRST HOUR

- ☐ The technical lead (Example IT Services on-call) resets the password and signs out all sessions for the account.
- ☐ The technical lead (Example IT Services on-call) checks and removes mail forwarding, inbox rules, added devices and new multi-factor methods.
- ☐ The incident lead (Morgan Sample) declares the level based on what the account could reach.
- ☐ The technical lead (Example IT Services on-call) checks other accounts for the same sign-in source.

FIRST DAY

- ☐ Review what the account accessed and sent while compromised.
- ☐ If the account is an administrator, treat all systems it manages as suspect.
- ☐ Legal counsel (Sample & Example LLP) advises if personal or regulated data was reachable.
- ☐ The communications lead (Jamie Example) warns anyone who received messages from the account.

RECOVER

- ☐ Enforce multi-factor authentication on the account and its peers.
- ☐ Remove access the account did not need.
- ☐ Brief the person on how the compromise happened.

DO NOT

- Do not only change the password; sessions and rules survive a password change.
- Do not assume one account is the whole story.

PLAYBOOK: LOST OR STOLEN DEVICE

How you will know: A laptop, phone or tablet holding company data is missing.

FIRST HOUR

- ☐ The person reports it to the technical lead (Example IT Services on-call) as soon as they notice.
- ☐ The technical lead (Example IT Services on-call) locks or wipes the device remotely and signs out its sessions.
- ☐ The technical lead (Example IT Services on-call) resets passwords for accounts used on the device.
- ☐ The incident lead (Morgan Sample) records what data was on the device and whether it was encrypted.

FIRST DAY

- ☐ File a police report if stolen.
- ☐ Legal counsel (Sample & Example LLP) advises on notification if the device was not encrypted and held personal data.
- ☐ Check for sign-ins from the device after it went missing.

RECOVER

- ☐ Replace the device from a standard build.
- ☐ Confirm encryption and remote wipe on all other devices.

DO NOT

- Do not wait a few days to see if it turns up before reporting it.

PLAYBOOK: VENDOR BREACH

How you will know: A vendor tells you, or you read in the news, that a company holding your data or access was breached.

FIRST HOUR

- ☐ The incident lead (Morgan Sample) records what the vendor said, when, and who said it.
- ☐ The technical lead (Example IT Services on-call) disables or restricts the vendor's access to your systems until the scope is known.
- ☐ The technical lead (Example IT Services on-call) changes any passwords, keys or tokens shared with the vendor.
- ☐ The incident lead (Morgan Sample) asks the vendor in writing what data of yours was involved and what they are doing.

FIRST DAY

- ☐ Legal counsel (Sample & Example LLP) reviews the contract for the vendor's duties and your own notification duties.
- ☐ The incident lead (Morgan Sample) notifies the insurer.
- ☐ Review your logs for activity from the vendor's accounts.
- ☐ The communications lead (Jamie Example) prepares a customer statement in case one is needed.

RECOVER

- ☐ Restore vendor access only after written confirmation of containment.
- ☐ Update the vendor's entry in the vendor risk review.

DO NOT

- Do not rely on the vendor's first statement; scope usually grows.
- Do not notify customers before counsel has reviewed the facts.

PLAYBOOK: DATA SENT OR EXPOSED BY MISTAKE

How you will know: An email with sensitive data went to the wrong person, or a file or folder was open to anyone with the link.

FIRST HOUR

- ☐ The person reports it to the incident lead (Morgan Sample) immediately; reporting fast is never punished.
- ☐ Recall the message if possible and ask the recipient in writing to delete it and confirm.
- ☐ The technical lead (Example IT Services on-call) removes public sharing and checks who opened the file.
- ☐ The incident lead (Morgan Sample) records what data, whose, how many people, and how long it was exposed.

FIRST DAY

- ☐ Legal counsel (Sample & Example LLP) advises whether notification is required.
- ☐ The incident lead (Morgan Sample) notifies the insurer if personal or regulated data was involved.
- ☐ The communications lead (Jamie Example) prepares a message for affected people if needed.

RECOVER

- ☐ Change sharing defaults to named people only.
- ☐ Add a send delay or a warning for outside recipients.

DO NOT

- Do not quietly fix it and move on. An unreported exposure is the bigger risk.

INCIDENT LOG

Start this the moment an incident is declared. One line per event, decision or action.

Date and time	What happened or was decided	By whom

KEEPING THIS PLAN CURRENT

- Review the plan at least once a year and after any incident. Next review: Oct 14, 2027.
- Check every phone number each quarter.
- Run a tabletop exercise at least once a year and record what was learned.
- Give a printed copy to every member of the response team. Copies are kept at: Front office safe; Dr. Example's home office; Example Security Partners case file.

EXERCISE HISTORY

Date	Scenario	Facilitator	Handled well	Partly	Gap	Action items
Oct 8, 2026	Ransomware: the Monday morning lockout	Alex Sample, Example Security Partners	1	2	1	5

APPROVAL

DR. R. EXAMPLE, OWNER

DATE