INCIDENT & SECURITY DISCOVERY INTAKE

Standardized first-call form

Use on the discovery call. Check what applies. Leave blanks. Do not collect passwords or MFA codes on this sheet.

Date / time _____	**DTS interviewer** _____	**Call type** [ ] Phone [ ] Video [ ] Onsite
Referred by _____	**Counsel / law firm on the call?** [ ] Yes [ ] No Name: _____	**File / job #** _____

1. Who is on this call — and who can decide

Primary contact / title

_____

Best phone + email

_____

Company legal name

_____

DBA / brand (if different)

_____

Role of the people on this call

[ ] Owner / partner
[ ] Office / practice manager
[ ] Internal IT / admin
[ ] Outside MSP / IT vendor
[ ] Counsel (their lawyer)
[ ] Insurer / broker / adjuster
[ ] CFO / controller / bookkeeper
[ ] Other: _____

Who can approve spend today? Name / title: _____

[ ] They are on this call [ ] We must wait for someone else [ ] Spend authority is unknown

Why now? [ ] Active emergency [ ] Suspected compromise [ ] After-action / cleanup [ ] Insurance / counsel asked [ ] Preventive / vCISO

2. Organization size, locations, industry

About how many people use computers / email here?

[ ] 1–10 [ ] 11–25 [ ] 26–50 [ ] 51–100
[ ] 101–200 [ ] 200+ [ ] Not sure

Rough counts (best guess is fine): Workstations _____ Servers _____ Locations _____ Remote users _____

HQ / primary address _____

Other sites (offices, plants, home offices that matter):

Industry / what the business actually does

[ ] Law / professional services
[ ] Healthcare / dental / therapy
[ ] Accounting / CPA / tax
[ ] Banking / credit union / lending
[ ] Insurance agency / broker
[ ] Defense / federal contractor
[ ] Manufacturer / industrial
[ ] Construction / trades
[ ] Nonprofit / church / school
[ ] Retail / e-commerce
[ ] Real estate / property mgmt
[ ] Other: _____

One-sentence description of the business _____

_____

3. Compliance, reporting, and data they hold

This changes the work, the paperwork, and whether we can be the only vendor. Ask even if they say "we're just a small shop."

Check every regime that might apply. If unsure, check "maybe" and write why.

Regime	Yes	Maybe	No	Notes / who asked
HIPAA / HITECH (PHI, ePHI, medical, dental, therapy, pharmacy)	[ ]	[ ]	[ ]	_____
GLBA / FTC Safeguards (banks, credit unions, lenders, many advisors)	[ ]	[ ]	[ ]	_____
DFARS / NIST 800-171 / CMMC / CUI (defense or federal subcontract)	[ ]	[ ]	[ ]	_____
Banking / NCUA / FFIEC / state banking exam	[ ]	[ ]	[ ]	_____
Accounting / CPA / tax prep (client returns, IRS Pub 4557, FTC)	[ ]	[ ]	[ ]	_____
Legal / ABA 1.6 / TN RPC 1.6 (attorney–client privilege)	[ ]	[ ]	[ ]	_____
PCI-DSS (they take cards themselves, not only Stripe/Square)	[ ]	[ ]	[ ]	_____
FERPA / student records (school, college, daycare with education $)	[ ]	[ ]	[ ]	_____
SOX / public-company or significant public-company vendor	[ ]	[ ]	[ ]	_____
State AG / breach-notification (TN, NC, or other — any PII)	[ ]	[ ]	[ ]	_____
Cyber insurer control requirements (MFA, EDR, backups) already in force	[ ]	[ ]	[ ]	_____
ITAR / export control / other: _____	[ ]	[ ]	[ ]	_____

What regulated data actually lives here?

[ ] Health / medical notes
[ ] Tax returns / SSNs
[ ] Bank / wire / ACH
[ ] Attorney–client files
[ ] CUI / government data
[ ] Cardholder data (PAN)
[ ] HR / employee records
[ ] Customer lists / PII
[ ] Not sure — need to find out
[ ] None they can name

Who do they have to notify if this is a reportable incident? [ ] Clients [ ] Insurer [ ] Regulator / AG [ ] Prime contractor [ ] Board [ ] Unknown

4. Cyber insurance (ask early — it changes who leads)

If a policy exists they should call the number on the declarations page. The carrier may require a panel forensic firm and a breach-coach lawyer. We can still contain and rebuild; we may not be the reimbursable DFIR vendor.

Do they have cyber / cyber-liability insurance?

[ ] Yes — policy in force
[ ] Yes — but unsure if this is covered
[ ] No policy
[ ] Don't know / will check
[ ] Only a general liability / package (probably not cyber)
[ ] Claim already opened

Carrier / broker name

_____

Policy # / renewal month

_____

Have they called the carrier yet? [ ] Yes [ ] No [ ] Broker is calling [ ] Told not to
Breach coach or panel IR firm already assigned? [ ] No [ ] Yes — name: _____
Deductible / they know it? $_____ [ ] Unknown [ ] They want us to work even if insurance will not pay us

Other insurance that might matter

[ ] E&O / professional liability
[ ] Crime / social-engineering / wire
[ ] Property / business interruption
[ ] None / unknown

5. What is happening right now

Symptoms they can name (check all)

[ ] Ransomware / files encrypted
[ ] Email sending as them / BEC
[ ] Microsoft 365 locked or strange
[ ] Backups failed or also encrypted
[ ] Customer data possibly taken
[ ] Law enforcement already involved
[ ] Cannot log into PCs / servers
[ ] Wire / ACH / payment fraud
[ ] VPN / RDP left open or abused
[ ] Website / WordPress hacked
[ ] Extortion / leak-site threat
[ ] Nothing live — preventive call

When did they first notice? _____ **Still getting worse?** [ ] Yes [ ] No [ ] Unknown

What still works? [ ] Email [ ] Phones [ ] Banking [ ] File share [ ] Line-of-business app [ ] Website [ ] Nothing

What must work this week to keep the lights on?

What have they already done?

[ ] Pulled network / Wi-Fi
[ ] Reset some passwords
[ ] Restored from backup
[ ] Called FBI / local PD / CISA
[ ] Nothing yet
[ ] Powered machines off
[ ] Paid or talked to attacker
[ ] Called another vendor
[ ] Told staff / clients
[ ] Not sure

If they paid or are negotiating: do not write amounts on this sheet. Note only that payment / contact occurred, then take it offline with counsel.

6. Environment snapshot (enough to size the work)

Identity / email

[ ] Microsoft 365 / Exchange Online
[ ] On-prem Exchange / AD only
[ ] No directory — local PCs
[ ] MFA on all users [ ] Yes [ ] No [ ] ?
[ ] Google Workspace
[ ] Mixed AD + 365
[ ] MFA on admins [ ] Yes [ ] No [ ] ?
[ ] Who is global admin? _____

Endpoints & servers

[ ] Windows workstations
[ ] Linux servers / VPS
[ ] WordPress / web host
[ ] QuickBooks / desktop accounting
[ ] Windows servers
[ ] Macs
[ ] Line-of-business app (name: _____)
[ ] Phone system / VoIP on same LAN

Network (who made it)

[ ] Ubiquiti / UniFi
[ ] Aruba
[ ] Consumer / ISP router only
[ ] Site-to-site VPN
[ ] SonicWall
[ ] Cisco / Meraki
[ ] Unknown / “the last guy”
[ ] Exposed RDP / VPN to internet

Who supports this today?

[ ] Nobody / owner does it
[ ] Outside MSP (name: _____)
[ ] Multiple vendors who don’t talk
[ ] Internal one-person IT
[ ] DTS already

EDR / antivirus in place? [ ] None [ ] Defender only [ ] Huntress / other EDR: _____ [ ] Unknown

7. Backups, identity, and whether we can restore

Backups exist? [ ] Yes [ ] “We think so” [ ] No [ ] Unknown
Last known-good restore that actually worked? Date: _____ [ ] Never tested [ ] Unknown

Where do backups live?

[ ] Local NAS / USB
[ ] Another server on the same LAN
[ ] Cloud (Wasabi / B2 / Azure / AWS)
[ ] M365 native / OneDrive only
[ ] Datto / Axcient / other BDR
[ ] Offline / air-gapped / immutable
[ ] Encrypted by the incident too
[ ] Unknown

Admin path we can use today (no passwords on this form): [ ] 365 admin they can sit with [ ] Server in the room [ ] VPN [ ] Hosting panel [ ] None yet

8. Access, logistics, and constraints

Can someone with admin rights stay on a screen-share in the next 24 hours? [ ] Yes [ ] After hours [ ] No
Onsite needed / wanted? [ ] Remote only [ ] Johnson City / Tri-Cities [ ] WNC [ ] Other: _____

Hours they operate
_____

Hard deadline (payroll, court, close, Monday)
_____

Customers / staff already asking? [ ] No [ ] Staff only [ ] Clients [ ] Press / public

Anything we must not touch? (production machine, camera system, medical device, CNC, etc.)

9. What they want from us (so we quote the right product)

[ ] Emergency contain + get operating
[ ] Full incident response + written findings
[ ] Stabilize / security overhaul after
[ ] WordPress cleanup only
[ ] Drive wipe / hardware disposal
[ ] Ongoing MSP / MSSP
[ ] vCISO / vCIO after this is over
[ ] CMMC / SPRS / DFARS help
[ ] Just a second opinion
[ ] They don't know — need us to say

Budget conversation (do not invent a number on the call)

[ ] Insurance expected to pay investigation
[ ] They will self-pay containment
[ ] Need a written SOW before any work
[ ] Need a mobilization / first-48-hours number today
[ ] Price is the main constraint
[ ] Speed is the main constraint

10. Internal — DTS only (do not send this page to the client)

Red flags

[ ] No spend authority on the call
[ ] Policy exists but they refuse to call carrier
[ ] Want us to wipe evidence / skip counsel
[ ] Already paid / still talking to attacker
[ ] No backups and no 365 admin
[ ] Regulated data + they want it quiet
[ ] Another vendor still "handling it"
[ ] Scope unclear after 30 minutes

Working size band (from the call, not a promise)

[ ] Tiny / first-48 only ($3–8k mobilization)
[ ] Small contain + restore
[ ] Mid IR + stabilize
[ ] Large / multi-site — or hand to panel DFIR
[ ] Not IR — MSP / vCISO / WP / destruction
[ ] Decline / refer

Next action we committed to

[ ] Send written SOW today
[ ] Join their carrier / counsel call
[ ] Remote session at: _____
[ ] Onsite at: _____
[ ] They will send: insurance dec page / org chart / admin on a call
[ ] No commitment — they will think

Use the margins or a second sheet for extra notes. Do not write passwords or payment amounts on this form.