Security awareness training evidence

Example Compliance Partners EC

Example Machining Co.

Managed by Example Compliance Partners · Generated Nov 15, 2026 at 23:49 UTC

SAMPLE. This company and its people are invented. Made by Arndel to show what a pack contains.

Complete	People	Courses done	Overdue
87%	**8**	**123 of 141**	**6 (1 person)**

140 completion records on file, including those of 1 former member, kept with their history. Records are append-only: a correction adds a voiding record rather than changing the original.

What this pack is: who was trained, on what, and when, laid out by the assessment objectives of NIST SP 800-171A, with the company's own training plan (which risks, which roles, who holds them) as it approved it. What it isn't: a judgment that those decisions are adequate, which is the assessor's to make. The roster is the people in this workspace: compare it with the company's own list of users. Dates are UTC.

Assessment objectives

AT.L2-3.2.1 Role-based risk awareness

3.2.1[a] Security risks associated with organizational activities involving CUI are identified. — Listed in this workspace

Shown here: The company's training plan (version 2, approved by Maria Alvarez (President) on 2026-07-20) identifies 12 risks in its work with CUI, with who each concerns. It is listed under Training plan.

The company adds: Whatever sits behind that list: your risk assessment or security plan.

3.2.1[b] Policies, standards, and procedures related to the security of the system are identified. — Listed in this workspace

Shown here: The security policies this workspace has listed for its people to read, with their versions.

The company adds: The policies, standards and procedures themselves.

3.2.1[c] Managers, systems administrators, and users of the system are made aware of the security risks associated with their activities. — Training records

Users (everyone): 6 of 8 current | Managers: 2 of 2 current | System administrators: 1 of 1 current

Shown here: Completions of the all-staff courses for each person, with the version of the content each one saw.

The company adds: Your list of system users, to compare with the roster here. Anyone missing from the roster has no record.

3.2.1[d] Managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system. — Training records

Users (everyone): 6 of 8 current | Managers: 2 of 2 current | System administrators: 1 of 1 current

Shown here: The policy sign-off: each person's dated statement that they have read the company's own policies, naming the ones listed. The courses teach the rules behind those policies.

The company adds: The policies, standards and procedures themselves.

AT.L2-3.2.2 Role-based training

3.2.2[a] Information security-related duties, roles, and responsibilities are defined. — Listed in this workspace

Shown here: The company's training plan (version 2, approved by Maria Alvarez (President) on 2026-07-20) defines 6 security roles and the duties of each. They are listed under Training plan.

The company adds: Anywhere else these roles are defined: your security plan or job descriptions.

3.2.2[b] Information security-related duties, roles, and responsibilities are assigned to designated personnel. — Listed in this workspace

Shown here: The company's training plan (version 2, approved by Maria Alvarez (President) on 2026-07-20) names who holds each security role, and the role tracks each person is on show who was designated for role training.

The company adds: Any assignment of security duties made outside this plan.

3.2.2[c] Personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities. — Training records

CUI handlers: 3 of 3 current | IT and system admins: 1 of 1 current | Executives: 1 of 1 current

Shown here: Completions of the role courses for each person on a role track, and any outside training recorded for them.

The company adds: Training for duties these courses don't cover, such as your own tools and procedures. Record it as outside training.

AT.L2-3.2.3 Insider threat awareness

3.2.3[a] Potential indicators associated with insider threats are identified. — Course content

Shown here: The indicators taught, listed with the insider threat courses under What was taught.
The company adds: Your insider threat policy or procedure, if it names indicators of its own.

3.2.3[b] Security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees. — Training records

Employees (everyone): 6 of 8 current | Managers: 2 of 2 current

Shown here: Completions of the insider threat courses by every employee, and of the managers' course by everyone who leads people.
The company adds: Your list of who manages people, to compare with the Managers track.

What the company tells its people

Shown to every learner inside the courses, and named in the policy sign-off. The policies themselves are held by the company.

Security reports go to	Tom Becker, IT and security lead - security@examplemachining.example or 555-0142, any hour. In person: the IT office by the tool crib.
CUI is allowed in	The CUI drive (the Contracts share), work email on a company laptop, and the locked cabinet in the quality office. Nowhere else.
Policies are kept	The Policies folder on the intranet, and a binder in the lunchroom
Policies to read	Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)
Last changed	Jun 18, 2026 by Maria Alvarez

Training plan

The company's own record of the decisions behind its training: the risks in its work with CUI, its security roles and who holds them. Written and approved by the company. It shows the decisions were made and when; whether they are adequate is for the assessor.

Version	2 of 2 (first approved Jun 18, 2026)
Approved	Jul 20, 2026 by Maria Alvarez, President
Recorded by	Maria Alvarez
Next review due	Jul 20, 2027
Fingerprint	SHA-256 28b0d6a69a511b15c39d7d8c9cfa23a7513ed03afc355be4966a7ededb43612e

Risks in the company's work with CUI (3.2.1[a])

Receiving and sending CUI by email
CUI is sent to the wrong person, forwarded to a personal account, or leaves the company without the protection the contract requires.
Concerns: All staff | Taught in: CUI in email and chat

Everyday email and messages
Someone is tricked into giving up a password, approving a sign-in or opening a malicious attachment.
Concerns: All staff | Taught in: Phishing aimed at suppliers, Passwords and two-step sign-in

Recognizing CUI when it arrives
CUI that is unmarked or badly marked isn't recognized, and is handled like ordinary paperwork.
Concerns: All staff, CUI handlers | Taught in: CUI basics, Marking CUI

USB drives and other removable media
A drive holding CUI is lost, or an unknown drive brings malware onto a system that holds it.
Concerns: All staff | Taught in: USB drives and removable media

Visitors, deliveries and the shop floor
Someone without a need to know sees or photographs CUI on a screen, a printout or a part.
Concerns: All staff | Taught in: Doors, desks and visitors

Noticing and reporting incidents

An incident isn't reported quickly enough for the company to contain it and meet its 72-hour reporting duty.

Concerns: All staff, IT and system admins | Taught in: Reporting incidents, Incident response for admins

People joining, moving and leaving

Someone with access takes or leaks information, or keeps access after they have left.

Concerns: Insider threat, Managers and supervisors | Taught in: Insider threat awareness, Insider threat: the warning signs, Insider threat for managers

Disposing of paper, drives and equipment

CUI leaves the company on paper, a drive or a machine that wasn't destroyed or sanitized.

Concerns: CUI handlers | Taught in: Destroying CUI

Administering the systems that hold CUI

An administrator account is misused or taken over, and nobody notices because the logs aren't kept or read.

Concerns: IT and system admins | Taught in: Admin accounts and privileged access, Logging and audit, Secure configuration and change

Affirming compliance each year

Leadership affirms a score or a status that the evidence doesn't support.

Concerns: Executives | Taught in: Leading on CMMC, The annual affirmation

Sending drawings to outside plating and heat-treat shops

A drawing marked CUI goes to a vendor who hasn't agreed to protect it, or goes with more detail than the job needs.

Concerns: CUI handlers, Managers and supervisors | Taught in: Handling CUI day to day

Using AI tools and online services

CUI is pasted or uploaded into a public AI tool or website that keeps it.

Concerns: All staff | Taught in: AI tools and CUI

Policies, standards and procedures (3.2.1[b])

Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)

Security roles, duties and who holds them (3.2.2[a], 3.2.2[b])

Senior official

Approves the security plan and this training plan, gives the program its budget and people, and affirms compliance each year.

Held by: Maria Alvarez | Training: Executives track

Security lead

Runs the security program day to day, takes security reports, and keeps the system security plan and plan of action current.

Held by: Tom Becker

System administrator

Administers the systems that hold CUI: accounts, configuration, patching, logging and remote access.

Held by: Tom Becker | Training: IT and system admins track

CUI handler

Receives, marks, stores, shares and destroys CUI in the course of their work.

Held by: Priya Nair, Lena Fischer, Dev Patel | Training: CUI handlers track

Manager or supervisor

Sees that their people finish their training, acts on concerns raised to them, and tells IT at once when someone leaves or changes role.

Held by: Maria Alvarez, Priya Nair, James Okafor | Training: Managers and supervisors track

All users

Follow the acceptable use rules, protect CUI as trained, and report anything suspicious straight away.

Held by: everyone on the roster | Training: All staff track

Named in the plan, but the training doesn't line up

James Okafor (Manager or supervisor) isn't on the Managers and supervisors track.

Courses by practice

Practice	Requirement	Courses	Current
AT.L2-3.2.1	Role-based risk awareness	Start here: security at a defense supplier, CUI basi...	90 of 104
AT.L2-3.2.2	Role-based training	FCI, CUI and everything else, Handling CUI day to...	19 of 19
AT.L2-3.2.3	Insider threat awareness	Insider threat awareness, Insider threat: the warnin...	14 of 18

Training by person

Person	Course	Status	Completed	Valid until	Version
Dev Patel dev.patel@examplemachining.example CUI handlers Started Feb 13, 2025	Start here: security at a defense s...	Complete	Jul 18, 2026		8aecc0d
	CUI basics	Complete	Jul 19, 2026		c94c47c
	Marking CUI	Complete	Jul 19, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 19, 2026		892f9ed
	Storing and sharing files	Complete	Jul 19, 2026		ee47e81
	AI tools and CUI	Complete	Jul 20, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Aug 11, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 20, 2026		e10f028
	USB drives and removable media	Complete	Jul 20, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 20, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 21, 2026		ca4f077
	Reporting incidents	Complete	Jul 21, 2026		7fee793
	Insider threat awareness	Complete	Jul 21, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 21, 2026		f49b77d
	FCI, CUI and everything else	Complete	Jul 22, 2026	Jul 22, 2027	3f51b34
	Handling CUI day to day	Complete	Jul 22, 2026	Jul 22, 2027	fc75b06
	CUI categories and who may recei...	Complete	Jul 22, 2026	Jul 22, 2027	2cccf55
	Destroying CUI	Complete	Jul 22, 2026	Jul 22, 2027	b214e81
	Policy sign-off	Complete	Jul 23, 2026	Jul 23, 2027	831556b
Grace Liu grace.liu@examplemachining.example Started Nov 6, 2026	Start here: security at a defense s...	Complete	Nov 11, 2026		8aecc0d
	CUI basics	Complete	Nov 12, 2026		c94c47c
	Marking CUI	Complete	Nov 12, 2026		beb8e9f
	CUI in email and chat	Due Dec 15, 2...			
	Storing and sharing files	Due Dec 15, 2...			
	AI tools and CUI	Due Dec 15, 2...			
	Phishing aimed at suppliers	Due Dec 15, 2...			
	Passwords and two-step sign-in	Due Dec 15, 2...			
	USB drives and removable media	Due Dec 15, 2...			
	Phones, home working and travel	Due Dec 15, 2...			
	Doors, desks and visitors	Due Dec 15, 2...			
	Reporting incidents	Due Dec 15, 2...			
	Insider threat awareness	Due Dec 15, 2...			
	Insider threat: the warning signs	Due Dec 15, 2...			
	Policy sign-off	Due Dec 15, 2...			

Person	Course	Status	Completed	Valid until	Version
James Okafor james.okafor@examplemachining.exam... Started Aug 3, 2023	Start here: security at a defense s...	Complete	Jul 20, 2026		8aecc0d
	CUI basics	Complete	Jul 21, 2026		c94c47c
	Marking CUI	Complete	Jul 21, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 21, 2026		892f9ed
	Storing and sharing files	Complete	Jul 21, 2026		ee47e81
	AI tools and CUI	Complete	Jul 22, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jul 22, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 22, 2026		e10f028
	USB drives and removable media	Complete	Sep 16, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 23, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 23, 2026		ca4f077
	Reporting incidents	Complete	Jul 23, 2026		7fee793
	Insider threat awareness	Complete	Jul 23, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 24, 2026		f49b77d
	Policy sign-off	Complete	Jul 24, 2026	Jul 24, 2027	831556b
Lena Fischer lena.fischer@examplemachining.example CUI handlers Started May 29, 2024	Start here: security at a defense s...	Complete	Jul 11, 2026		8aecc0d
	CUI basics	Complete	Jul 12, 2026		c94c47c
	Marking CUI	Complete	Jul 12, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 12, 2026		892f9ed
	Storing and sharing files	Complete	Jul 12, 2026		ee47e81
	AI tools and CUI	Complete	Jul 13, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jul 13, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 13, 2026		e10f028
	USB drives and removable media	Complete	Jul 13, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 14, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 14, 2026		ca4f077
	Reporting incidents	Complete	Jul 14, 2026		7fee793
	Insider threat awareness	Complete	Jul 14, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 15, 2026		f49b77d
	FCI, CUI and everything else	Complete	Jul 15, 2026	Jul 15, 2027	3f51b34
	Handling CUI day to day	Complete	Jul 15, 2026	Jul 15, 2027	fc75b06
	CUI categories and who may recei...	Complete	Jul 15, 2026	Jul 15, 2027	2cccf55
	Destroying CUI	Complete	Jul 16, 2026	Jul 16, 2027	b214e81
	Policy sign-off	Complete	Jul 16, 2026	Jul 16, 2027	831556b

Person	Course	Status	Completed	Valid until	Version
Maria Alvarez maria.alvarez@examplemachining.exa... Managers and supervisors, Executives Started Dec 7, 2018	Start here: security at a defense s...	Complete	Jun 26, 2026		8aecc0d
	CUI basics	Complete	Jun 27, 2026		c94c47c
	Marking CUI	Complete	Jun 27, 2026		beb8e9f
	CUI in email and chat	Complete	Jun 27, 2026		892f9ed
	Storing and sharing files	Complete	Jun 27, 2026		ee47e81
	AI tools and CUI	Complete	Jun 28, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jun 28, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jun 28, 2026		e10f028
	USB drives and removable media	Complete	Jun 28, 2026		854a0e8
	Phones, home working and travel	Complete	Jun 29, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jun 29, 2026		ca4f077
	Reporting incidents	Complete	Jun 29, 2026		7fee793
	Insider threat awareness	Complete	Jun 29, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jun 30, 2026		f49b77d
	Insider threat for managers	Complete	Jun 30, 2026	Jun 30, 2027	a667cd4
	Leading on CMMC	Complete	Jun 30, 2026	Jun 30, 2027	4894703
	The annual affirmation	Complete	Jun 30, 2026	Jun 30, 2027	2864b33
	Policy sign-off	Complete	Jul 1, 2026	Jul 1, 2027	831556b
Priya Nair priya.nair@examplemachining.example Managers and supervisors, CUI handlers Started Feb 14, 2021	Start here: security at a defense s...	Complete	Jul 7, 2026		8aecc0d
	CUI basics	Complete	Jul 8, 2026		c94c47c
	Marking CUI	Complete	Jul 8, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 8, 2026		892f9ed
	Storing and sharing files	Complete	Jul 8, 2026		ee47e81
	AI tools and CUI	Complete	Jul 9, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jul 9, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 9, 2026		e10f028
	USB drives and removable media	Complete	Jul 9, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 10, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 10, 2026		ca4f077
	Reporting incidents	Complete	Jul 10, 2026		7fee793
	Insider threat awareness	Complete	Jul 10, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 11, 2026		f49b77d
	Insider threat for managers	Complete	Jul 11, 2026	Jul 11, 2027	a667cd4
	FCI, CUI and everything else	Complete	Jul 11, 2026	Jul 11, 2027	3f51b34
	Handling CUI day to day	Complete	Jul 11, 2026	Jul 11, 2027	fc75b06
	CUI categories and who may recei...	Complete	Jul 12, 2026	Jul 12, 2027	2cccf55
	Destroying CUI	Complete	Jul 12, 2026	Jul 12, 2027	b214e81
	Policy sign-off	Complete	Jul 12, 2026	Jul 12, 2027	831556b

Person	Course	Status	Completed	Valid until	Version
Ruth Novak ruth.novak@examplemachining.example Former member since Oct 6, 2026 Started Mar 21, 2022	Start here: security at a defense s...	Complete	Jul 3, 2026		8aecc0d
	CUI basics	Complete	Jul 4, 2026		c94c47c
	Marking CUI	Complete	Jul 4, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 4, 2026		892f9ed
	Storing and sharing files	Complete	Jul 4, 2026		ee47e81
	AI tools and CUI	Complete	Jul 5, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jul 5, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 5, 2026		e10f028
	USB drives and removable media	Complete	Jul 5, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 6, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 6, 2026		ca4f077
	Reporting incidents	Complete	Jul 6, 2026		7fee793
	Insider threat awareness	Complete	Jul 6, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 7, 2026		f49b77d
	Policy sign-off	Complete	Jul 7, 2026	Jul 7, 2027	831556b
Sam Whitaker sam.whitaker@examplemachining.exa... Started Oct 1, 2025	Start here: security at a defense s...	Complete	Sep 24, 2026		8aecc0d
	CUI basics	Complete	Sep 25, 2026		c94c47c
	Marking CUI	Complete	Sep 25, 2026		beb8e9f
	CUI in email and chat	Complete	Sep 25, 2026		892f9ed
	Storing and sharing files	Complete	Sep 25, 2026		ee47e81
	AI tools and CUI	Complete	Sep 26, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Sep 26, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Sep 26, 2026		e10f028
	USB drives and removable media	Complete	Sep 26, 2026		854a0e8
	Phones, home working and travel	Overdue			
	Doors, desks and visitors	Overdue			
	Reporting incidents	Overdue			
	Insider threat awareness	Overdue			
	Insider threat: the warning signs	Overdue			
	Policy sign-off	Overdue			

Person	Course	Status	Completed	Valid until	Version
Tom Becker tom.becker@examplemachining.example IT and system admins Started Oct 7, 2022	Start here: security at a defense s...	Complete	Jun 30, 2026		8aecc0d
	CUI basics	Complete	Jul 1, 2026		c94c47c
	Marking CUI	Complete	Jul 1, 2026		beb8e9f
	CUI in email and chat	Complete	Jul 1, 2026		892f9ed
	Storing and sharing files	Complete	Jul 1, 2026		ee47e81
	AI tools and CUI	Complete	Jul 2, 2026		c4bbf5d
	Phishing aimed at suppliers	Complete	Jul 2, 2026		4e29fd3
	Passwords and two-step sign-in	Complete	Jul 2, 2026		e10f028
	USB drives and removable media	Complete	Jul 2, 2026		854a0e8
	Phones, home working and travel	Complete	Jul 3, 2026		1a4d3e8
	Doors, desks and visitors	Complete	Jul 3, 2026		ca4f077
	Reporting incidents	Complete	Jul 3, 2026		7fee793
	Insider threat awareness	Complete	Jul 3, 2026		cc8c368
	Insider threat: the warning signs	Complete	Jul 4, 2026		f49b77d
	Admin accounts and privileged ac...	Complete	Jul 4, 2026	Jul 4, 2027	db7f3f7
	Logging and audit	Complete	Jul 4, 2026	Jul 4, 2027	c06f15b
	Secure configuration and change	Complete	Jul 4, 2026	Jul 4, 2027	388faa4
	Remote access and outside conn...	Complete	Jul 5, 2026	Jul 5, 2027	484b900
	Incident response for admins	Complete	Jul 5, 2026	Jul 5, 2027	b03251f
	Policy sign-off	Complete	Jul 5, 2026	Jul 5, 2027	831556b

Completion records

Person	Course	Date	Score	Acknowledged as	Record
Maria Alvarez	Start here: security at a defe...	Jun 26, 2026	5/5	Maria Alvarez	0c89ff9a
Maria Alvarez	CUI basics	Jun 27, 2026	6/6	Maria Alvarez	48dce630
Maria Alvarez	Marking CUI	Jun 27, 2026	6/6	Maria Alvarez	a1e8780d
Maria Alvarez	CUI in email and chat	Jun 27, 2026	6/6	Maria Alvarez	4782210f
Maria Alvarez	Storing and sharing files	Jun 27, 2026	6/6	Maria Alvarez	de739a00
Maria Alvarez	AI tools and CUI	Jun 28, 2026	6/6	Maria Alvarez	6de32699
Maria Alvarez	Phishing aimed at suppliers	Jun 28, 2026	7/7	Maria Alvarez	a2e0b792
Maria Alvarez	Passwords and two-step sign...	Jun 28, 2026	6/6	Maria Alvarez	e8ded470
Maria Alvarez	USB drives and removable m...	Jun 28, 2026	6/6	Maria Alvarez	5f1f3699
Maria Alvarez	Phones, home working and t...	Jun 29, 2026	6/6	Maria Alvarez	d6a9cb6a
Maria Alvarez	Doors, desks and visitors	Jun 29, 2026	6/6	Maria Alvarez	b123d534
Maria Alvarez	Reporting incidents	Jun 29, 2026	7/7	Maria Alvarez	e4f04b5f
Maria Alvarez	Insider threat awareness	Jun 29, 2026	6/6	Maria Alvarez	09a17cfc
Maria Alvarez	Insider threat: the warning si...	Jun 30, 2026	7/7	Maria Alvarez	5ad6dfa1
Maria Alvarez	Insider threat for managers	Jun 30, 2026	8/8	Maria Alvarez	9adf91b6
Maria Alvarez	Leading on CMMC	Jun 30, 2026	7/7	Maria Alvarez	9565584f
Tom Becker	Start here: security at a defe...	Jun 30, 2026	5/5	Tom Becker	4b479960
Maria Alvarez	The annual affirmation	Jun 30, 2026	8/8	Maria Alvarez	ac677070
Maria Alvarez	Policy sign-off	Jul 1, 2026	4/4	Maria Alvarez	4788407d
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Tom Becker	CUI basics	Jul 1, 2026	6/6	Tom Becker	9511b9ba
Tom Becker	Marking CUI	Jul 1, 2026	6/6	Tom Becker	082d50e0
Tom Becker	CUI in email and chat	Jul 1, 2026	6/6	Tom Becker	33be75a8
Tom Becker	Storing and sharing files	Jul 1, 2026	6/6	Tom Becker	75168ed0

Person	Course	Date	Score	Acknowledged as	Record
Tom Becker	AI tools and CUI	Jul 2, 2026	6/6	Tom Becker	c65ede67
Tom Becker	Phishing aimed at suppliers	Jul 2, 2026	7/7	Tom Becker	3da2b2b1
Tom Becker	Passwords and two-step sign...	Jul 2, 2026	6/6	Tom Becker	e36f6ccc
Tom Becker	USB drives and removable m...	Jul 2, 2026	6/6	Tom Becker	af9a41aa
Tom Becker	Phones, home working and t...	Jul 3, 2026	6/6	Tom Becker	649b3318
Tom Becker	Doors, desks and visitors	Jul 3, 2026	6/6	Tom Becker	673f7196
Tom Becker	Reporting incidents	Jul 3, 2026	7/7	Tom Becker	b61dc9d8
Ruth Novak	Start here: security at a defe...	Jul 3, 2026	5/5	Ruth Novak	e1adf495
Tom Becker	Insider threat awareness	Jul 3, 2026	6/6	Tom Becker	cfe5d1dd
Ruth Novak	CUI basics	Jul 4, 2026	6/6	Ruth Novak	05025dec
Tom Becker	Insider threat: the warning si...	Jul 4, 2026	7/7	Tom Becker	f7286bdb
Tom Becker	Admin accounts and privileg...	Jul 4, 2026	9/9	Tom Becker	f031eb35
Ruth Novak	Marking CUI	Jul 4, 2026	6/6	Ruth Novak	4d54de2e
Ruth Novak	CUI in email and chat	Jul 4, 2026	6/6	Ruth Novak	eb832843
Tom Becker	Logging and audit	Jul 4, 2026	8/8	Tom Becker	809bb4e7
Ruth Novak	Storing and sharing files	Jul 4, 2026	6/6	Ruth Novak	e1d992b6
Tom Becker	Secure configuration and ch...	Jul 4, 2026	9/9	Tom Becker	1cfdf030
Tom Becker	Remote access and outside ...	Jul 5, 2026	8/8	Tom Becker	354dc424
Ruth Novak	AI tools and CUI	Jul 5, 2026	6/6	Ruth Novak	ab44cfa2
Ruth Novak	Phishing aimed at suppliers	Jul 5, 2026	7/7	Ruth Novak	019bd97a
Tom Becker	Incident response for admins	Jul 5, 2026	9/9	Tom Becker	f8ed86dd
Tom Becker	Policy sign-off	Jul 5, 2026	4/4	Tom Becker	3fdcca3d
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Ruth Novak	Passwords and two-step sign...	Jul 5, 2026	6/6	Ruth Novak	def15d54
Ruth Novak	USB drives and removable m...	Jul 5, 2026	6/6	Ruth Novak	32bdde3f
Ruth Novak	Phones, home working and t...	Jul 6, 2026	6/6	Ruth Novak	ad22ba8e
Ruth Novak	Doors, desks and visitors	Jul 6, 2026	6/6	Ruth Novak	b1677b94
Ruth Novak	Reporting incidents	Jul 6, 2026	7/7	Ruth Novak	8bc3aab1
Ruth Novak	Insider threat awareness	Jul 6, 2026	6/6	Ruth Novak	7f9caa12
Ruth Novak	Insider threat: the warning si...	Jul 7, 2026	7/7	Ruth Novak	2b5a872b
Ruth Novak	Policy sign-off	Jul 7, 2026	4/4	Ruth Novak	42119886
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Priya Nair	Start here: security at a defe...	Jul 7, 2026	5/5	Priya Nair	ec8e541f
Priya Nair	CUI basics	Jul 8, 2026	6/6	Priya Nair	057e3d34
Priya Nair	Marking CUI	Jul 8, 2026	6/6	Priya Nair	910478c1
Priya Nair	CUI in email and chat	Jul 8, 2026	6/6	Priya Nair	5cee897f
Priya Nair	Storing and sharing files	Jul 8, 2026	6/6	Priya Nair	e17890b1
Priya Nair	AI tools and CUI	Jul 9, 2026	6/6	Priya Nair	50c90194
Priya Nair	Phishing aimed at suppliers	Jul 9, 2026	7/7	Priya Nair	86ea54a6
Priya Nair	Passwords and two-step sign...	Jul 9, 2026	6/6	Priya Nair	7017c136
Priya Nair	USB drives and removable m...	Jul 9, 2026	6/6	Priya Nair	27f0c695
Priya Nair	Phones, home working and t...	Jul 10, 2026	6/6	Priya Nair	7b5aad57
Priya Nair	Doors, desks and visitors	Jul 10, 2026	6/6	Priya Nair	00830ae6
Priya Nair	Reporting incidents	Jul 10, 2026	7/7	Priya Nair	a128c566
Priya Nair	Insider threat awareness	Jul 10, 2026	6/6	Priya Nair	30f99343

Person	Course	Date	Score	Acknowledged as	Record
Priya Nair	Insider threat: the warning si...	Jul 11, 2026	7/7	Priya Nair	249c01dc
Priya Nair	Insider threat for managers	Jul 11, 2026	8/8	Priya Nair	cb176929
Priya Nair	FCI, CUI and everything else	Jul 11, 2026	7/7	Priya Nair	40b15e7d
Lena Fischer	Start here: security at a defe...	Jul 11, 2026	5/5	Lena Fischer	e2e0deca
Priya Nair	Handling CUI day to day	Jul 11, 2026	7/7	Priya Nair	6e0dfb83
Lena Fischer	CUI basics	Jul 12, 2026	6/6	Lena Fischer	dfb27d42
Priya Nair	CUI categories and who may...	Jul 12, 2026	8/8	Priya Nair	a3d49d2c
Priya Nair	Destroying CUI	Jul 12, 2026	8/8	Priya Nair	05195d40
Lena Fischer	Marking CUI	Jul 12, 2026	6/6	Lena Fischer	d6a23ede
Lena Fischer	CUI in email and chat	Jul 12, 2026	6/6	Lena Fischer	f09d6bad
Priya Nair	Policy sign-off	Jul 12, 2026	4/4	Priya Nair	7fb32454
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Lena Fischer	Storing and sharing files	Jul 12, 2026	6/6	Lena Fischer	e4e69547
Lena Fischer	AI tools and CUI	Jul 13, 2026	6/6	Lena Fischer	4284821f
Lena Fischer	Phishing aimed at suppliers	Jul 13, 2026	7/7	Lena Fischer	08355bfc
Lena Fischer	Passwords and two-step sign...	Jul 13, 2026	6/6	Lena Fischer	a5e78b96
Lena Fischer	USB drives and removable m...	Jul 13, 2026	6/6	Lena Fischer	c6e03d88
Lena Fischer	Phones, home working and t...	Jul 14, 2026	6/6	Lena Fischer	73dd5fc6
Lena Fischer	Doors, desks and visitors	Jul 14, 2026	6/6	Lena Fischer	872aef34
Lena Fischer	Reporting incidents	Jul 14, 2026	7/7	Lena Fischer	82357b0e
Lena Fischer	Insider threat awareness	Jul 14, 2026	6/6	Lena Fischer	795cd4cb
Lena Fischer	Insider threat: the warning si...	Jul 15, 2026	7/7	Lena Fischer	678a3628
Lena Fischer	FCI, CUI and everything else	Jul 15, 2026	7/7	Lena Fischer	a2b7e87f
Lena Fischer	Handling CUI day to day	Jul 15, 2026	7/7	Lena Fischer	1c8806ec
Lena Fischer	CUI categories and who may...	Jul 15, 2026	8/8	Lena Fischer	db9f12f9
Lena Fischer	Destroying CUI	Jul 16, 2026	8/8	Lena Fischer	1d4105fb
Lena Fischer	Policy sign-off	Jul 16, 2026	4/4	Lena Fischer	ef5ba00c
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Dev Patel	Start here: security at a defe...	Jul 18, 2026	5/5	Dev Patel	dd90a7fd
Dev Patel	CUI basics	Jul 19, 2026	6/6	Dev Patel	308db8b1
Dev Patel	Marking CUI	Jul 19, 2026	6/6	Dev Patel	46b3aa9a
Dev Patel	CUI in email and chat	Jul 19, 2026	6/6	Dev Patel	ef3d736e
Dev Patel	Storing and sharing files	Jul 19, 2026	6/6	Dev Patel	60de229b
Dev Patel	AI tools and CUI	Jul 20, 2026	6/6	Dev Patel	34bfd838
Dev Patel	Passwords and two-step sign...	Jul 20, 2026	6/6	Dev Patel	06d72123
Dev Patel	USB drives and removable m...	Jul 20, 2026	6/6	Dev Patel	adc36e5a
James Okafor	Start here: security at a defe...	Jul 20, 2026	5/5	James Okafor	5fc0e7cd
Dev Patel	Phones, home working and t...	Jul 20, 2026	6/6	Dev Patel	7b91c6aa
James Okafor	CUI basics	Jul 21, 2026	6/6	James Okafor	f9c184e7
Dev Patel	Doors, desks and visitors	Jul 21, 2026	6/6	Dev Patel	0a38902a
James Okafor	Marking CUI	Jul 21, 2026	6/6	James Okafor	81b5761f
Dev Patel	Reporting incidents	Jul 21, 2026	7/7	Dev Patel	0633113b
James Okafor	CUI in email and chat	Jul 21, 2026	6/6	James Okafor	6f15a5e6
Dev Patel	Insider threat awareness	Jul 21, 2026	6/6	Dev Patel	1936e494
Dev Patel	Insider threat: the warning si...	Jul 21, 2026	7/7	Dev Patel	7213a667

Person	Course	Date	Score	Acknowledged as	Record
James Okafor	Storing and sharing files	Jul 21, 2026	6/6	James Okafor	52fde17e
James Okafor	AI tools and CUI	Jul 22, 2026	6/6	James Okafor	5684ff29
Dev Patel	FCI, CUI and everything else	Jul 22, 2026	7/7	Dev Patel	2697c2cd
James Okafor	Phishing aimed at suppliers	Jul 22, 2026	7/7	James Okafor	5e87de6c
Dev Patel	Handling CUI day to day	Jul 22, 2026	7/7	Dev Patel	0114ffd2
James Okafor	Passwords and two-step sign...	Jul 22, 2026	6/6	James Okafor	358d9361
Dev Patel	CUI categories and who may...	Jul 22, 2026	8/8	Dev Patel	592df2ed
James Okafor	USB drives and removable m...	Jul 22, 2026	6/6	James Okafor	0b579a46 (voided)
Dev Patel	Destroying CUI	Jul 22, 2026	8/8	Dev Patel	35a7c589
James Okafor	Phones, home working and t...	Jul 23, 2026	6/6	James Okafor	896d150b
Dev Patel	Policy sign-off	Jul 23, 2026	4/4	Dev Patel	6af099d4
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
James Okafor	Doors, desks and visitors	Jul 23, 2026	6/6	James Okafor	6a9320ed
James Okafor	Reporting incidents	Jul 23, 2026	7/7	James Okafor	0771fa49
James Okafor	Insider threat awareness	Jul 23, 2026	6/6	James Okafor	484e9045
James Okafor	Insider threat: the warning si...	Jul 24, 2026	7/7	James Okafor	a4328764
James Okafor	Policy sign-off	Jul 24, 2026	4/4	James Okafor	0ef43357
	Signed for: Acceptable Use Policy (v4, March 2026); CUI Handling Procedure (v2, January 2026); Incident Reporting Procedure (v3, March 2026); Removable Media Policy (v2, June 2025)				
Dev Patel	Phishing and social engineer...	Aug 11, 2026		Example Security T...	93f79dca
James Okafor	USB drives and removable m...	Sep 16, 2026	6/6	James Okafor	f1124d7f
Sam Whitaker	Start here: security at a defe...	Sep 24, 2026	5/5	Sam Whitaker	f731d7fd
Sam Whitaker	CUI basics	Sep 25, 2026	6/6	Sam Whitaker	8180cd4a
Sam Whitaker	Marking CUI	Sep 25, 2026	6/6	Sam Whitaker	3c2fcbb1
Sam Whitaker	CUI in email and chat	Sep 25, 2026	6/6	Sam Whitaker	c9617b20
Sam Whitaker	Storing and sharing files	Sep 25, 2026	6/6	Sam Whitaker	10d9f984
Sam Whitaker	AI tools and CUI	Sep 26, 2026	6/6	Sam Whitaker	60123f3f
Sam Whitaker	Phishing aimed at suppliers	Sep 26, 2026	7/7	Sam Whitaker	e718f3fe
Sam Whitaker	Passwords and two-step sign...	Sep 26, 2026	6/6	Sam Whitaker	7535e6a0
Sam Whitaker	USB drives and removable m...	Sep 26, 2026	6/6	Sam Whitaker	22224943
Grace Liu	Start here: security at a defe...	Nov 11, 2026	5/5	Grace Liu	8d63cb46
Grace Liu	CUI basics	Nov 12, 2026	6/6	Grace Liu	a3f7bfc5
Grace Liu	Marking CUI	Nov 12, 2026	6/6	Grace Liu	ec355233
James Okafor	Void: USB drives and remova...	Nov 15, 2026			57719e3c

What was taught

Each version of a course that a record in this pack names, and the current version of anything still to be taken. The version is a fingerprint of everything a learner sees or is graded on: a change to the wording makes a new one. Quiz questions and answers are held by Arndel and aren't printed here.

Start here: security at a defense supplier

Version 8aecc0d, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 9 standing records | 5 questions, 80% to pass

After it, a person can	Say why a small supplier is a target; Tell contract information apart from everything else you handle; Use the five habits from your first day; Know who to ask and how to report
Pages	Why you are doing this; Two kinds of information to know; Five habits from day one; Who to ask, and what happens next
Rules cited	DFARS 252.204-7012; NIST SP 800-171 Rev. 2, 3.2.1; FAR 52.204-21 (numbered 52.240-93 in contracts written under the 2026 FAR overhaul); 32 CFR 2002.4(h); NIST SP 800-171 Rev. 2, 3.1.10, 3.1.20, 3.6.2 and 3.10.3; NIST SP 800-171 Rev. 2, 3.2.1 and 3.6.2; DFARS 252.204-7012(c)
Statement signed	I understand that my company handles information for the U.S. government that must be protected. I will keep it on company systems, ask when I am unsure, and report security concerns and my own mistakes promptly.
Kept current	Taken once, then kept current by the annual refresher.

CUI basics

Version c94c47c, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 9 standing records | 6 questions, 80% to pass

After it, a person can	Explain what CUI is in your own words; Recognize CUI when it is marked, and suspect it when it isn't; Say why losing it matters to your company; Apply the three rules: approved systems, need for the work, report
Pages	What CUI is; How you recognize it; Why it matters; Your part: three rules
Rules cited	32 CFR 2002.4(h) and 2002.18; DFARS 252.204-7012(a); 32 CFR 2002.20; DoD Instruction 5230.24; DFARS 252.204-7012(b); 32 CFR 170.16 and 170.22; NIST SP 800-171 Rev. 2, 3.2.1; NIST SP 800-171 Rev. 2, 3.1.1, 3.1.3 and 3.1.20
Statement signed	I understand what Controlled Unclassified Information is. I will keep it on the systems my company has approved for it, share it only with people who need it for the work, and report anything that looks wrong.
Kept current	Taken once, then kept current by the annual refresher.

Marking CUI

Version beb8e9f, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 9 standing records | 6 questions, 80% to pass

After it, a person can	Read a CUI banner and a designation block; Keep markings on copies, excerpts, emails and media; Know what to do with legacy or missing markings
Pages	What markings are for; Reading the banner; The designation block; Markings travel with the information; Legacy and missing markings
Rules cited	32 CFR 2002.20; NIST SP 800-171 Rev. 2, 3.8.4; 32 CFR 2002.20(b); DoD Instruction 5200.48; 32 CFR 2002.20(d); 32 CFR 2002.36; 32 CFR 2002.20(a) and (i); 32 CFR 2002.16(a)
Statement signed	I will keep CUI markings on the copies, excerpts, emails and media I create. I will not remove a marking, or decide on my own whether unmarked information is CUI, and I will tell my security lead when a marking is missing or unclear.
Kept current	Taken once, then kept current by the annual refresher.

CUI in email and chat

Version 892f9ed, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 8 standing records | 6 questions, 80% to pass

After it, a person can	Check the recipient and the channel before sending; Mark an email that contains CUI; Respond properly to a misdirected or unexpected CUI email; Apply the same rules to chat, text and photos
Pages	Where CUI leaks; Before you send; Marking the message; When it goes wrong; Chat, text and photos
Rules cited	NIST SP 800-171 Rev. 2, 3.1.3; NIST SP 800-171 Rev. 2, 3.13.8 and 3.1.3; 32 CFR 2002.20; DoD Instruction 5200.48; NIST SP 800-171 Rev. 2, 3.6.2; NIST SP 800-171 Rev. 2, 3.1.18 and 3.1.20
Statement signed	I will send CUI only to people who need it for the work, only through the channels my company has approved, and marked as CUI. I will not use personal email or personal messaging for it, or any device my company has not approved for it, and I will report misdirected messages at once.
Kept current	Taken once, then kept current by the annual refresher.

Storing and sharing files

Version ee47e81, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 8 standing records | 6 questions, 80% to pass

After it, a person can	Tell an approved location from a convenient one; Share inside the company without widening access; Know what has to be true before a file goes to a supplier; Keep contract information off public channels
Pages	Approved locations; Sharing inside the company; Sharing with suppliers and customers; Never in public
Rules cited	NIST SP 800-171 Rev. 2, 3.1.3 and 3.1.20; DFARS 252.204-7012(b)(2)(ii)(D); NIST SP 800-171 Rev. 2, 3.1.1, 3.1.2 and 3.1.5; DFARS 252.204-7012(m) and 252.204-7021(f); 32 CFR 170.23; NIST SP 800-171 Rev. 2, 3.1.3; NIST SP 800-171 Rev. 2, 3.1.22; DFARS 252.204-7000
Statement signed	I will store CUI only in the locations my company has approved, I will not widen access to it or send it outside the company without approval, and I will not post or publish information about contract work without permission.
Kept current	Taken once, then kept current by the annual refresher.

AI tools and CUI

Version c4bbf5d, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 8 standing records | 6 questions, 80% to pass

After it, a person can	Explain why pasting into an AI tool is sharing; Spot the AI features that capture information without being asked; Use approved tools for the right tasks; Recognize AI-assisted scams
Pages	Pasting is sharing; The rule; AI that doesn't ask first; Using AI well; AI on the other side
Rules cited	NIST SP 800-171 Rev. 2, 3.1.20 and 3.1.3; NIST SP 800-171 Rev. 2, 3.1.20; DFARS 252.204-7012(b)(2)(ii)(D); FAR 52.204-21(b)(1)(iii); NIST SP 800-171 Rev. 2, 3.4.9 and 3.13.12; 32 CFR 2002.4(h); NIST SP 800-171 Rev. 2, 3.2.1
Statement signed	I will not put CUI or other contract information into any AI tool, extension or online service that my company has not approved for it, and I will verify unusual requests through a channel I already trust.
Kept current	Taken once, then kept current by the annual refresher.

Phishing aimed at suppliers

Version 4e29fd3, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c] | 8 standing records | 7 questions, 80% to pass

After it, a person can	Spot the signs in a message that looks legitimate; Recognize the versions aimed at suppliers: fake portals, RFQs and payment changes; Verify a request through a channel you already trust; Report a phish, including one you clicked
Pages	Why it works; The signs; Beyond email; What to do
Rules cited	NIST SP 800-171 Rev. 2, 3.2.1; NIST SP 800-171 Rev. 2, 3.2.1 and 3.5.3; NIST SP 800-171 Rev. 2, 3.6.2
Statement signed	I will check unexpected messages before acting on them, verify unusual requests through a channel I already trust, never share my password or sign-in codes, and report suspicious messages, including ones I have acted on.
Kept current	Taken once, then kept current by the annual refresher.

Passwords and two-step sign-in

Version e10f028, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 8 standing records | 6 questions, 80% to pass

After it, a person can	Make a password that resists guessing and reuse attacks; Use two-step sign-in without being talked out of it; Explain why accounts are never shared
Pages	How passwords fail; A password that holds; Two-step sign-in; One person, one account
Rules cited	NIST SP 800-171 Rev. 2, 3.2.1; NIST SP 800-63B-4, 3.1.1; NIST SP 800-171 Rev. 2, 3.5.2 and 3.5.7; NIST SP 800-171 Rev. 2, 3.5.3; NIST SP 800-171 Rev. 2, 3.1.10, 3.3.2 and 3.5.1
Statement signed	I will use a unique password for my work account, keep it and my sign-in codes to myself, approve only the sign-ins I start, lock my screen when I step away, and report any sign-in I did not start.
Kept current	Taken once, then kept current by the annual refresher.

USB drives and removable media

Version 854a0e8, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 8 standing records | 6 questions, 80% to pass

After it, a person can	Use only media the company issued or approved; Handle CUI on media: encrypted, marked and accounted for; Move programs to shop-floor machines the approved way; Hand media back at the end of its life
Pages	Two risks in one small object; Only the company's own; When CUI goes on media; On the shop floor; End of life
Rules cited	NIST SP 800-171 Rev. 2, 3.8.7; NIST SP 800-171 Rev. 2, 3.8.7 and 3.8.8; NIST SP 800-171 Rev. 2, 3.8.1, 3.8.4, 3.8.5 and 3.8.6; NIST SP 800-171 Rev. 2, 3.1.21 and 3.13.11; NIST SP 800-171 Rev. 2, 3.8.5 and 3.8.7; NIST SP 800-171 Rev. 2, 3.8.3
Statement signed	I will use only removable media my company has issued or approved, I will never connect unknown or personal devices to company systems, I will keep CUI media encrypted, marked and locked away, and I will report lost media and return old media for destruction.
Kept current	Taken once, then kept current by the annual refresher.

Phones, home working and travel

Version 1a4d3e8, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 7 standing records | 6 questions, 80% to pass

After it, a person can	Know which devices may connect to company systems; Set up a home workspace that protects what's on the screen; Travel with company devices safely; Ask before taking technical data abroad
Pages	Phones and tablets; Working from home; On the road; Travel abroad; Lost or stolen
Rules cited	NIST SP 800-171 Rev. 2, 3.1.18 and 3.1.19; NIST SP 800-171 Rev. 2, 3.10.6 and 3.1.12; NIST SP 800-171 Rev. 2, 3.1.12, 3.1.13 and 3.13.8; ITAR, 22 CFR 120.50; EAR, 15 CFR 734.13; NIST SP 800-171 Rev. 2, 3.6.2
Statement signed	I will use only approved devices and connections for work, protect my screen and papers wherever I work, tell my security lead before traveling abroad with company equipment, and report a lost or stolen device immediately.
Kept current	Taken once, then kept current by the annual refresher.

Doors, desks and visitors

Version ca4f077, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 7 standing records | 6 questions, 80% to pass

After it, a person can	Follow and enforce the visitor rules; Keep screens and paper out of view; Look after badges, keys and codes; Prepare a work area for a tour or a photograph
Pages	The building is a control; Visitors; What can be seen; Badges, keys and codes; Tours and photographs
Rules cited	NIST SP 800-171 Rev. 2, 3.10.1, 3.10.2 and 3.10.4; NIST SP 800-171 Rev. 2, 3.10.3 and 3.10.4; NIST SP 800-171 Rev. 2, 3.1.10 and 3.8.1; NIST SP 800-171 Rev. 2, 3.10.5; NIST SP 800-171 Rev. 2, 3.10.3 and 3.1.22
Statement signed	I will follow my company's visitor and access rules, challenge or report people who are unescorted where they shouldn't be, keep controlled work out of view, look after my badge, keys and codes, and not photograph work areas without permission.
Kept current	Taken once, then kept current by the annual refresher.

Reporting incidents

Version 7fee793, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[c], 3.2.1[d] | 7 standing records | 7 questions, 80% to pass

After it, a person can	Recognize the things that need reporting; Explain why the first hour matters; Make a report someone can act on; Avoid destroying evidence by trying to help
Pages	What to report; Why speed matters; How to report; What not to do; Reporting your own mistake
Rules cited	NIST SP 800-171 Rev. 2, 3.6.1 and 3.6.2; DFARS 252.204-7012(c) and (m); NIST SP 800-171 Rev. 2, 3.6.2; DFARS 252.204-7012(e); NIST SP 800-171 Rev. 2, 3.6.1; NIST SP 800-171 Rev. 2, 3.2.1
Statement signed	I know how to report a security incident at my company. I will report suspected incidents and my own mistakes immediately, from a safe device, and I will not delete, switch off or investigate anything on my own.
Kept current	Taken once, then kept current by the annual refresher.

Insider threat awareness

Version cc8c368, Nov 15, 2026 (current wording)

Insider threat | AT.L2-3.2.3, 3.2.3[a], 3.2.3[b] | 7 standing records | 6 questions, 80% to pass

After it, a person can	Describe an insider threat without assuming malice; Tell careless, compromised and deliberate insiders apart; Report a concern through the right route
Pages	What an insider threat is; Three kinds of insider; Why defense work raises the stakes; Reporting a concern
Rules cited	NIST SP 800-171 Rev. 2, 3.2.3; NIST SP 800-171 Rev. 2, 3.2.3 (discussion)
Statement signed	I understand what an insider threat is and that most are unintentional. I will report potential indicators and unusual approaches to my security lead or manager, sticking to what I saw or heard.
Kept current	Taken once, then kept current by the annual refresher.

Insider threat: the warning signs

Version f49b77d, Nov 15, 2026 (current wording)

Insider threat | AT.L2-3.2.3, 3.2.3[a], 3.2.3[b] | 7 standing records | 7 questions, 80% to pass

After it, a person can	List the indicators that relate to access and information; Weigh a single sign against a pattern; Avoid treating who someone is as a sign; Describe what happens after a report
Pages	Signs in how someone handles information; Signs in behavior and circumstances; One sign isn't a case; What is not a sign; After you report
Rules cited	NIST SP 800-171 Rev. 2, 3.2.3 (discussion); CMMC Assessment Guide, Level 2, AT.L2-3.2.3; NIST SP 800-171 Rev. 2, 3.2.3; NIST SP 800-171 Rev. 2, 3.2.3 and 3.6.2
Statement signed	I can recognize potential insider threat indicators and I understand that who a person is never counts as one. I will report conduct that concerns me to my security lead, and I won't gossip about what I report. I understand this doesn't limit my right to report to the government.
Kept current	Taken once, then kept current by the annual refresher.

Insider threat for managers

Version a667cd4, Nov 15, 2026 (current wording)

Managers and supervisors | AT.L2-3.2.3, 3.2.3[a], 3.2.3[b] | 2 standing records | 8 questions, 80% to pass

After it, a person can	Recognize the moments when risk is highest in a team; Handle a concern brought to you without investigating it yourself; Make sure access changes when a person's job does; Run a team where people report early
Pages	Why managers get their own course; The risky moments; When a concern reaches you; Joiners, movers and leavers; The team you run
Rules cited	NIST SP 800-171 Rev. 2, 3.2.3 (discussion); NIST SP 800-171A, 3.2.3[b]; NIST SP 800-171 Rev. 2, 3.2.3 and 3.6.2; NIST SP 800-171 Rev. 2, 3.9.2, 3.1.1 and 3.1.5; NIST SP 800-171 Rev. 2, 3.2.1 and 3.2.3
Statement signed	As a manager, I will pass concerns about potential insider threats to my security lead promptly without investigating them myself, tell IT and HR in time when people join, move or leave, and support my team in reporting mistakes and concerns.
Kept current	Retaken every 12 months.

FCI, CUI and everything else

Version 3f51b34, Nov 15, 2026 (current wording)

CUI handlers | AT.L2-3.2.2, 3.2.2[c] | 3 standing records | 7 questions, 80% to pass

After it, a person can	Define FCI and CUI and say what each requires; Recognize information that is neither; Find out which a piece of information is, starting from the contract; Carry the right status onto what you create
Pages	Three piles; What each requires; What is not CUI; Finding out; What you create
Rules cited	FAR 52.204-21(a) (numbered 52.240-93 in contracts written under the 2026 FAR overhaul); 32 CFR 2002.4(h); FAR 52.204-21(b); DFARS 252.204-7012(b); DFARS 252.204-7012(m); 32 CFR 2002.20; 32 CFR 2002.18 and 2002.20; NIST SP 800-171 Rev. 2, 3.8.4
Statement signed	I can tell FCI, CUI and other information apart. I will check the contract and markings rather than assume, protect unclear information as CUI until it is confirmed, and store and mark what I create according to what it contains.
Kept current	Retaken every 12 months.

Handling CUI day to day

Version fc75b06, Nov 15, 2026 (current wording)

CUI handlers | AT.L2-3.2.2, 3.2.2[c] | 3 standing records | 7 questions, 80% to pass

After it, a person can	Bring incoming CUI into the right system from the start; Work with CUI on screen, on paper and in conversation; Send CUI physically without advertising it; Keep working copies under control
Pages	Receiving; Using it; Talking about it; Shipping and carrying; Working copies
Rules cited	NIST SP 800-171 Rev. 2, 3.1.3 and 3.8.1; 32 CFR 2002.4(f) and 2002.14(c); DoD Instruction 5200.48 (after-hours storage); NIST SP 800-171 Rev. 2, 3.8.1; 32 CFR 2002.14(c); 32 CFR 2002.14(d) and 2002.20(i); NIST SP 800-171 Rev. 2, 3.8.5 and 3.8.6; NIST SP 800-171 Rev. 2, 3.8.1 and 3.8.2
Statement signed	I will receive, store, use, discuss and ship CUI as my company's CUI handling procedures require: in controlled environments, on approved systems, locked away when not in use, and with working copies kept to what the job needs.
Kept current	Retaken every 12 months.

CUI categories and who may receive them

Version 2cccf55, Nov 15, 2026 (current wording)

CUI handlers | AT.L2-3.2.2, 3.2.2[c] | 3 standing records | 8 questions, 80% to pass

After it, a person can	Explain CUI Basic and CUI Specified; Recognize Controlled Technical Information and export-controlled data; Read a distribution statement and a dissemination control; Stop before sharing technical data with a foreign person
Pages	Basic and Specified; Controlled Technical Information; Distribution statements; Dissemination controls; Export control and foreign persons
Rules cited	32 CFR 2002.4(j) and (r); 32 CFR 2002.14; DoD Instruction 5200.48; DFARS 252.204-7012(a); CUI Registry (archives.gov/cui); DoD Instruction 5230.24; 32 CFR 2002.16(a); 32 CFR 2002.16(b); ITAR, 22 CFR 120.50; EAR, 15 CFR 734.13
Statement signed	I understand the CUI categories my work involves. I will read distribution statements and dissemination controls before sharing, I will not work around them, and I will use my company's export compliance process before export-controlled data reaches any person or place I do not know to be cleared for it.
Kept current	Retaken every 12 months.

Destroying CUI

Version b214e81, Nov 15, 2026 (current wording)

CUI handlers | AT.L2-3.2.2, 3.2.2[c] | 3 standing records | 8 questions, 80% to pass

After it, a person can	Check that destruction is allowed before destroying; Destroy paper so it can't be reconstructed; Hand electronic media to the people who sanitize it; Treat scrap parts and tooling as information
Pages	Before you destroy anything; Paper; Files and media; Parts, tooling and scrap; When a contract ends
Rules cited	32 CFR 2002.14(f); ISOO CUI Notice 2019-03; NIST SP 800-171 Rev. 2, 3.8.3; NIST SP 800-171 Rev. 2, 3.8.3 and 3.7.3; NIST SP 800-88 Rev. 2; Your contract's scrap, demilitarization and property terms; ITAR, 22 CFR 120.50; DFARS 252.204-7012(m)
Statement signed	I will check that CUI may be destroyed before destroying it, use only the destruction methods my company has approved, hand media and equipment that has held CUI to IT for sanitization, and follow the scrap procedure for controlled parts and tooling.
Kept current	Retaken every 12 months.

Admin accounts and privileged access

Version db7f3f7, Nov 15, 2026 (current wording)

IT and system admins | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 9 questions, 80% to pass

After it, a person can	Keep privileged work in a separate account; Grant the least access that does the job, and review it; Manage shared, service and emergency accounts without losing accountability; Remove access promptly when people move or leave
Pages	Why your account is the target; Two accounts, used for different things; Least privilege, including yours; Sign-in for privileged accounts; Joiners, movers and leavers; Sign-in settings you set for everyone
Rules cited	NIST SP 800-171 Rev. 2, 3.1.5, 3.1.6 and 3.1.7; NIST SP 800-171 Rev. 2, 3.1.6 and 3.1.7; NIST SP 800-171 Rev. 2, 3.1.4, 3.1.5 and 3.3.9; NIST SP 800-171 Rev. 2, 3.5.1, 3.5.2 and 3.5.3; NIST SP 800-171 Rev. 2, 3.5.5, 3.5.6, 3.9.2 and 3.1.1; NIST SP 800-171 Rev. 2, 3.1.8, 3.1.10 and 3.5.4; NIST SP 800-171 Rev. 2, 3.5.7 to 3.5.10; NIST SP 800-63B-4, 3.1.1
Statement signed	I will use privileged access only for administrative tasks and from a separate account, grant the least access

	needed, never share or reuse administrative credentials, and remove access promptly when people change roles or leave.
Kept current	Retaken every 12 months.

Logging and audit

Version c06f15b, Nov 15, 2026 (current wording)

IT and system admins | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 8 questions, 80% to pass

After it, a person can	Decide which events need logging and confirm they are; Keep logs attributable, time-aligned and tamper-resistant; Review logs on a schedule and act on logging failures; Retain enough to investigate an incident found late
Pages	What logs are for; What to capture; Logs you can trust; When logging stops; Review and retention
Rules cited	NIST SP 800-171 Rev. 2, 3.3.1 and 3.3.2; DFARS 252.204-7012(c); NIST SP 800-171 Rev. 2, 3.3.1 and 3.3.3; NIST SP 800-171 Rev. 2, 3.3.7, 3.3.8 and 3.3.9; NIST SP 800-171 Rev. 2, 3.3.4 and 3.14.6; NIST SP 800-171 Rev. 2, 3.3.1, 3.3.5 and 3.3.6; DFARS 252.204-7012(e)
Statement signed	I will keep audit logging enabled, attributable, time-synchronized and protected on the systems I manage, alert on and investigate logging failures, review logs on the schedule my company's policy sets, and preserve evidence when an incident is suspected.
Kept current	Retaken every 12 months.

Secure configuration and change

Version 388faa4, Nov 15, 2026 (current wording)

IT and system admins | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 9 questions, 80% to pass

After it, a person can	Maintain baselines and an inventory you can show; Run changes through review, approval and a record; Reduce what each system can do to what it needs to do; Patch and scan on a schedule, and verify cryptography is validated
Pages	Baselines and inventory; Change control; Least functionality; Patching, scanning and malware protection; FIPS-validated cryptography; The network boundary
Rules cited	NIST SP 800-171 Rev. 2, 3.4.1 and 3.4.2; 32 CFR 170.19(c), Table 3; NIST SP 800-171 Rev. 2, 3.4.3, 3.4.4 and 3.4.5; NIST SP 800-171 Rev. 2, 3.4.6, 3.4.7, 3.4.8 and 3.4.9; NIST SP 800-171 Rev. 2, 3.14.1 to 3.14.5; NIST SP 800-171 Rev. 2, 3.11.2 and 3.11.3; 32 CFR 170.4 and 170.19(c); NIST SP 800-171 Rev. 2, 3.13.11, 3.13.8, 3.13.10 and 3.13.16; 32 CFR 170.4 (temporary deficiency); NIST SP 800-171 Rev. 2, 3.13.1, 3.13.5 and 3.13.6
Statement signed	I will build and maintain systems to documented baselines, make changes only through my company's change process, keep systems to the functions they need, apply fixes and scans on the schedule our policy sets, and verify that cryptography protecting CUI is FIPS-validated.
Kept current	Retaken every 12 months.

Remote access and outside connections

Version 484b900, Nov 15, 2026 (current wording)

IT and system admins | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 8 questions, 80% to pass

After it, a person can	Route remote access through managed, monitored points; Apply encryption and MFA to remote sessions, with split tunneling prevented; Control vendor and maintenance access; Handle mobile devices and external systems that touch CUI
Pages	The front door you chose; A proper remote session; Vendors and maintenance; Mobile devices and external systems; Wireless
Rules cited	NIST SP 800-171 Rev. 2, 3.1.12, 3.1.13, 3.1.14 and 3.5.3; NIST SP 800-171 Rev. 2, 3.1.7, 3.1.11, 3.1.13 and 3.1.15; NIST SP 800-171 Rev. 2, 3.5.3, 3.13.7, 3.13.9 and 3.13.11; NIST SP 800-171 Rev. 2, 3.7.2 to 3.7.6; NIST SP 800-171 Rev. 2, 3.1.18 to 3.1.21; DFARS 252.204-7012(b)(2)(ii)(D); NIST SP 800-171 Rev. 2, 3.1.16 and 3.1.17
Statement signed	I will allow remote access only through my company's managed access points, with encryption and multi-factor authentication, I will control and end vendor and maintenance access, and I will not connect external or unmanaged systems to CUI.
Kept current	Retaken every 12 months.

Incident response for admins

Version b03251f, Nov 15, 2026 (current wording)

IT and system admins | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 9 questions, 80% to pass

After it, a person can	Have the plan, contacts and reporting access ready in advance; Contain an incident without destroying evidence; Support the 72-hour report with facts; Test the plan and learn from each incident
Pages	What has to exist beforehand; The first hours; The reporting clock; Recovery; Testing and learning
Rules cited	NIST SP 800-171 Rev. 2, 3.6.1, 3.6.2 and 3.6.3; DFARS 252.204-7012(c)(3); NIST SP 800-171 Rev. 2, 3.6.1; DFARS 252.204-7012(c), (d), (e), (f) and (m)(2); NIST SP 800-171 Rev. 2, 3.6.1 and 3.8.9; DFARS 252.204-7012(e); NIST SP 800-171 Rev. 2, 3.6.3
Statement signed	I will follow my company's incident response plan: alert the incident lead at once, contain by isolating, preserve evidence and logs, support the 72-hour report with facts, and take part in testing the plan.
Kept current	Retaken every 12 months.

Leading on CMMC

Version 4894703, Nov 15, 2026 (current wording)

Executives | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 7 questions, 80% to pass

After it, a person can	Explain the requirements and how they are verified; Make the scoping, resourcing and role decisions that belong to leadership; Read the company's score and plan of action honestly; Oversee the program through a short set of regular questions
Pages	What the company has agreed to; Decisions only you can make; Reading the score honestly; Your supply chain, both ways; Oversight in practice
Rules cited	FAR 52.204-21 (numbered 52.240-93 in solicitations since February 2026); DFARS 252.204-7012 and 252.204-7020(f); 32 CFR Part 170; DFARS Class Deviation 2026-O0025; NIST SP 800-171 Rev. 2, 3.2.2, 3.11.1 and 3.12.2; 32 CFR 170.19; NIST SP 800-171 Rev. 2, 3.12.2 and 3.12.4; 32 CFR 170.21 and 170.24; DFARS 252.204-7012(b)(2)(ii)(D) and (m); DFARS 252.204-7021(d) and (f); 32 CFR 170.19(c)(2) and 170.23; NIST SP 800-171 Rev. 2, 3.12.1 and 3.12.3
Statement signed	I understand my company's obligations to protect FCI and CUI and my responsibility to define security roles, resource them, approve the plan of action, and oversee the program through regular reporting.
Kept current	Retaken every 12 months.

The annual affirmation

Version 2864b33, Nov 15, 2026 (current wording)

Executives | AT.L2-3.2.2, 3.2.2[c] | 1 standing record | 8 questions, 80% to pass

After it, a person can	Say what the affirmation attests and when it is made; Understand the exposure a false affirmation creates; Assemble the evidence a signature should rest on; Know what to do when the statement wouldn't be true
Pages	What you are signing; Why the signature matters; What should be on your desk; When it wouldn't be true; Staying affirmable all year
Rules cited	32 CFR 170.22; False Claims Act, 31 U.S.C. 3729 to 3733; NIST SP 800-171 Rev. 2, 3.12.1 and 3.12.4; 32 CFR 170.4, 170.21, 170.22 and 170.24; DFARS 252.204-7021(a) and (d); NIST SP 800-171 Rev. 2, 3.12.3
Statement signed	I understand that the annual affirmation is a statement to the government that my company has implemented and is maintaining its security requirements. I will review the evidence behind it before it is made, and I will not affirm what the evidence does not support.
Kept current	Retaken every 12 months.

Policy sign-off

Version 831556b, Nov 15, 2026 (current wording)

All staff | AT.L2-3.2.1, 3.2.1[d] | 7 standing records | 4 questions, 75% to pass

After it, a person can	Name the security policies that apply to you and where to find them; Explain what your signature commits you to
Pages	The policies behind the training; Before you sign; What your signature means
Rules cited	NIST SP 800-171 Rev. 2, 3.2.1; NIST SP 800-171A, 3.2.1[d]
Statement signed	I know where my company's security policies are kept. I have read the policies, standards and procedures that apply to my role, including the ones my company has listed for this sign-off. I will follow them, and I will ask my manager or security lead when I am unsure.
Kept current	Retaken every 12 months.