AUGMENTIVE BUSINESS 7 SOLUTIONS PVT. LTD.

COMPLIANCE CHECKLISTS

Data Security & Confidentiality Agreement Template

Ready-to-use NDA and confidentiality templates for remote staff. Includes IP assignment and security protocols.

Executive Summary

Remote workers pose data security risks. This document provides ready-to-use NDA and confidentiality agreement templates, IP assignment clauses, and security acknowledgment forms. Customize these templates with your company details (in [BRACKETS]) and require all remote staff to sign before accessing company data.

91%	$4.5M	3 Days	100%
Of breaches involve remote workers	Average data breach cost	Average time to detect breach	Staff must sign agreements

How to Use These Templates

Overview

This section provides five ready-to-use legal agreements and policies that protect your company's intellectual property and confidential information when working with remote contractors and employees worldwide.

Customization Steps:

1. Read through each template completely
2. Identify all [BRACKET] sections that require your company information
3. Replace [COMPANY NAME] with your legal entity name
4. Replace [EFFECTIVE DATE] with the agreement start date
5. Have an attorney in your state review and approve
6. Print, sign, and have worker sign both copies
7. Maintain original signed copies in your employee file
8. Send worker a copy for their records

Legal Notice:

> **Disclaimer**
> These templates are provided for reference only and should not be considered legal advice. Every company's situation is unique. Have an employment attorney in your jurisdiction review these templates before use to ensure compliance with state and local laws.

Template 1: Master Non-Disclosure Agreement (NDA)

This is a comprehensive NDA that covers confidentiality of trade secrets, business information, and client data. Use this as your standard agreement for all remote workers.

NDA – Non-Disclosure Agreement

This Agreement is made and entered into effective as of [EFFECTIVE DATE] (the "Effective Date") by and between [COMPANY NAME], a [STATE] corporation ("Company"), and [WORKER NAME], an individual ("Worker").

1. CONFIDENTIAL INFORMATION

Worker acknowledges that in the course of employment/engagement with Company, Worker will have access to and become acquainted with various trade secrets and confidential business information owned or controlled by Company, including but not limited to:

- Client lists, customer data, and contact information
- Pricing information, cost structures, and financial data
- Business plans, strategies, and marketing approaches
- Technical information, software code, and systems architecture
- Internal processes, procedures, and operational methods
- Proprietary research, analysis, and methodologies
- Health information and protected health information (PHI)
- Personal data of any individual (PII)

(Collectively, "Confidential Information").

2. OBLIGATIONS OF WORKER

Worker agrees to:

- Maintain all Confidential Information in strict confidence
- Use Confidential Information only for the purpose of performing assigned work
- Limit disclosure to employees or contractors who have a legitimate need to know
- Not disclose Confidential Information to any third party without prior written consent
- Not remove, photograph, copy, or transcribe Confidential Information without authorization
- Return all Confidential Information upon request or termination
- Employ security measures consistent with industry standards
- Report any unauthorized access or suspected breach within 24 hours

3. EXCLUSIONS FROM CONFIDENTIALITY

Confidential Information does not include information that:

- Is already in the public domain or becomes public without breach by Worker
- Was rightfully known to Worker prior to disclosure (with documentation)
- Is rightfully received from a third party without confidentiality restrictions
- Is independently developed by Worker without reference to Confidential Information

However, Worker must provide prompt written notice of any claimed exclusion.

4. TERM AND DURATION

This NDA is effective as of the Effective Date and continues during Worker's engagement and for [5] years after termination, except that obligations regarding trade secrets continue indefinitely.

5. RETURN OF MATERIALS

Upon request or termination of engagement, Worker shall immediately return or destroy (at Company's election) all Confidential Information, including:

- Physical documents and files
- Electronic copies, emails, and messages
- Notes, summaries, or transcriptions
- Photos, videos, or recordings

Worker shall certify in writing that all Confidential Information has been returned or destroyed.

6. NO LICENSE OR RIGHTS

This NDA grants Worker no license or rights in the Confidential Information. All Confidential Information remains the exclusive property of Company.

7. NO OBLIGATION TO DISCLOSE

Company is under no obligation to disclose any Confidential Information to Worker. Company may modify or discontinue access at any time.

8. REMEDIES

Worker acknowledges that breach of this NDA would cause irreparable harm for which monetary damages are an inadequate remedy. Company shall have the right to seek injunctive relief in addition to all other remedies.

9. GOVERNING LAW

This NDA shall be governed by and construed in accordance with the laws of [STATE], without regard to conflicts of law principles.

Template 2: Intellectual Property Assignment Agreement

This agreement ensures that all work product created by the worker becomes the property of your company. This is critical for software developers, content creators, designers, and anyone producing intellectual property.

IP Assignment Agreement

This Agreement is made effective as of [EFFECTIVE DATE] by and between [COMPANY NAME] ("Company") and [WORKER NAME] ("Worker").

1. ASSIGNMENT OF WORK PRODUCT

Worker agrees that all work, work product, inventions, discoveries, and intellectual property ("Work Product") created, developed, or produced by Worker during the course of engagement with Company, whether during work hours or using Company resources, shall be the exclusive property of Company.

This includes:

- Software code, algorithms, and technical documentation
- Written content, documentation, and communications
- Designs, graphics, and creative works
- Concepts, methodologies, and processes
- Data, databases, and analysis
- Any modifications or improvements to existing Company systems

2. PRIOR INVENTIONS

Worker may list any prior inventions or intellectual property created before engagement on Exhibit A attached. These items are excluded from this assignment.

3. ASSIGNMENT OF RIGHTS

Worker hereby assigns to Company all right, title, and interest in and to all Work Product, including:

- All intellectual property rights (patents, copyrights, trademarks, trade secrets)
- All derivative and moral rights
- All rights to register and enforce such rights

4. COOPERATION

Worker agrees to:

- Execute any documents necessary to perfect Company's title to Work Product
- Assist in obtaining and enforcing patents, copyrights, or trademarks
- Provide testimony or declarations regarding Work Product
- Not challenge Company's ownership or register conflicting claims

5. NO COMPENSATION BEYOND FEES

Except for the agreed fee, Worker shall receive no additional compensation for the assignment of Work Product, including any royalties, residuals, or ongoing payments.

6. CONFIDENTIALITY OF WORK PRODUCT

Worker acknowledges that Work Product is Confidential Information and shall maintain strict confidentiality.

Template 3: Data Security Policy Acknowledgment

Require all remote workers to sign this acknowledgment confirming they understand data security obligations.

Data Security Policy Acknowledgment

I, [WORKER NAME], acknowledge that I have read, understand, and agree to comply with [COMPANY NAME]'s Data Security Policy.

My Obligations Include:

- Using only [COMPANY NAME]-approved devices and software
- Maintaining strong passwords and changing them every 90 days
- Enabling multi-factor authentication (MFA) on all accounts
- Never sharing login credentials or access tokens
- Locking my device when away from my desk, even briefly
- Using only encrypted connections (VPN when on public networks)
- Not installing unauthorized software or apps
- Not connecting personal USB drives or external media
- Not printing or photographing documents without authorization
- Not sharing screens during calls with client data visible
- Reporting suspicious emails (phishing) immediately
- Reporting any suspected security incident within 24 hours
- Completing security training annually
- Not working from public locations (coffee shops, airports) with sensitive data
- Disposing of confidential documents securely (shredding or burning)

Consequences of Non-Compliance:

I understand that violation of the Data Security Policy may result in:

- Suspension of system access
- Disciplinary action up to and including termination
- Legal action to recover damages
- Personal liability for breach costs

Signature Block:

Employee/Contractor Signature: _____ Date: _____

Manager/HR Signature: _____ Date: _____

Template 4: Device and System Access Agreement

Use this agreement to define acceptable use of company-provided or company-accessed systems and devices.

Device and System Access Agreement

1. COMPANY-PROVIDED DEVICES

If Company provides a laptop, phone, or other device, Worker acknowledges:

- Device remains property of Company at all times
- Company may monitor, inspect, or audit the device without notice
- Device will be returned in good condition upon termination
- Worker is responsible for damage beyond normal wear and tear

2. SYSTEM ACCESS

Worker shall only access systems and data for authorized business purposes. Unauthorized access is strictly prohibited.

3. MONITORING AND LOGGING

Worker acknowledges and consents to:

- Logging of all system access and data viewing
- Recording of internet activity and website visits
- Email scanning and archiving
- Video recording of workspace during work hours (if applicable)
- Periodic security audits and assessments

Worker has no expectation of privacy in Company systems or devices.

4. PERSONAL USE

Personal use of Company systems must be minimal and during authorized breaks only. Company reserves the right to prohibit personal use entirely.

5. REMOVAL OF DATA

Worker shall not:

- Copy, download, or transfer Company data to personal devices
- Print or photograph Company data
- Share login credentials with family or friends
- Sync Company email with personal devices (unless approved)

6. TERMINATION OF ACCESS

Upon termination, Company will immediately:

- Disable Worker's system access
- Collect all devices
- Retrieve any data stored on personal devices

- Reset or wipe devices containing Company data

Template 5: Incident Reporting Protocol

Establish a clear protocol for workers to report security incidents. Quick reporting is critical to minimize breach damage.

Data Incident Reporting Protocol

1. WHAT TO REPORT

Worker must immediately report any of the following:

- Suspected unauthorized access to Company systems or data
- Lost or stolen devices containing Company data
- Phishing emails or social engineering attempts
- Suspicious activity in Company accounts
- Exposure of Confidential Information to unauthorized persons
- Malware, viruses, or security alerts on devices
- Accidental disclosure or misconfiguration
- Breaches or incidents at third-party vendors

2. HOW TO REPORT

Report immediately by:

- Email: [SECURITY EMAIL ADDRESS]
- Phone: [SECURITY PHONE NUMBER]
- Slack/Teams: [SECURITY CHANNEL]

Do NOT wait until end of day or next business day. Report immediately, even if you are uncertain.

3. INCIDENT REPORT FORMAT

Include the following information:

- Date and time of incident or discovery
- Type of incident (data loss, unauthorized access, phishing, etc.)
- Systems or data affected
- Number of records or individuals potentially impacted
- How the incident was discovered
- Current status (ongoing or contained)
- Actions already taken
- Recommended next steps

4. INVESTIGATION PROCESS

After reporting:

9. Security team will investigate within 2 hours
10. Affected systems may be isolated or shut down
11. Worker may be asked for additional information

12. Worker should not discuss incident with colleagues unless authorized
13. Company will determine if incident is reportable to regulators

5. NO RETALIATION

Worker is protected from retaliation for good-faith incident reporting. Reports will not result in disciplinary action unless Worker was negligent or violated policy.

State-Specific Customization Notes

California

California courts favor strong confidentiality and non-compete limitations. Add this language: "This agreement does not prevent Worker from disclosing Confidential Information when required by law or court order, provided Worker gives Company notice and cooperates in seeking a protective order."

New York

New York requires reasonable non-competes. If including non-compete language, ensure it is narrowly tailored. Recommend: "Worker agrees not to solicit Company's customers for [1] year post-termination in the [state] region."

Florida

Florida law is employer-friendly for NDAs. Include explicit language on trade secret protection and remedies for breach.

Texas

Texas Uniform Trade Secrets Act applies. Include this language: "Company treats all Confidential Information as trade secrets under the Texas Uniform Trade Secrets Act, and Worker acknowledges that breach may result in injunctive relief."

International (India, etc.)

Add language: "This agreement shall be governed by [Company State] law. Worker consents to jurisdiction in [County/State] courts. Worker shall comply with both US and [Country] privacy and data protection laws."

Customization Guide: Fill-in-the-Blank Sections

Identify All [BRACKET] Fields:

Bracket Field	Required Information	Example
[COMPANY NAME]	Your legal entity name	AB7 Solutions PVT. LTD.
[EFFECTIVE DATE]	Start date of agreement	January 15, 2026
[WORKER NAME]	Full legal name of worker	John David Smith
[STATE]	State of incorporation / jurisdiction	New York
[5] years	Duration of confidentiality obligation	3-10 years (tailor to your business)
[SECURITY EMAIL ADDRESS]	Email for incident reporting	security@ab7solutions.com
[SECURITY PHONE NUMBER]	Phone for incident reporting	+1-321-341-7733
[SECURITY CHANNEL]	Internal messaging channel	#security-incidents (Slack)
[APPROVED DEVICES]	Devices worker can use	Company laptop, approved phone only
[APPROVED SOFTWARE]	Permitted applications list	See Appendix A

Sample Signed Agreement Checklist

Before allowing any remote worker to access data, ensure:

- ✓ NDA is printed, signed by worker and manager, dated
- ✓ IP Assignment Agreement is signed (if applicable)
- ✓ Data Security Policy Acknowledgment is signed
- ✓ Device and System Access Agreement is signed
- ✓ Incident Reporting Protocol is reviewed (verbal acknowledgment acceptable)
- ✓ Worker has received a copy of each signed agreement
- ✓ Original signed copies are stored in personnel file
- ✓ Copies are provided to worker for their records
- ✓ All agreements are dated within 30 days of engagement start
- ✓ International workers have country-specific addenda signed

Enforcement Best Practices

Signing agreements is only the first step. Enforce them:

Ongoing Compliance:

- Review agreements annually and update as needed
- Conduct security awareness training for all remote staff quarterly
- Run simulated phishing tests and track results
- Log all system access and regularly audit logs
- Implement technical controls (VPN, encryption, MFA)

When Breaches Occur:

- Investigate fully and document findings
- Determine if breach was intentional or negligent
- Take appropriate disciplinary action
- Consider legal action for serious breaches
- Update agreements to close loopholes

Documentation:

- Maintain signed copies for 7+ years after worker departure
- Keep incident reports and investigation files
- Document all training completion and test results
- Record all security communications and updates

Customization Checklist: Before Using Templates

Complete this checklist before deploying any agreement:

- ✓ Have employment attorney review all templates for your state
- ✓ Obtain approval from your CEO/General Counsel
- ✓ Fill in all [BRACKET] sections with company-specific information
- ✓ Add any state-specific addenda or modifications
- ✓ Format consistently (logo, branding, colors)
- ✓ Include table of contents and page numbers
- ✓ Prepare two printed copies for each worker
- ✓ Create a tracking log of signed agreements by worker
- ✓ Set up secure storage for signed originals
- ✓ Establish a review schedule (annually)
- ✓ Communicate policy changes to existing staff

About AB7 Solutions

AB7 Solutions provides pre-made security agreements and manages compliance for remote workers. All our staff sign comprehensive NDAs, IP assignments, and security acknowledgments. We maintain secure document handling and incident reporting protocols compliant with HIPAA, GDPR, and data protection laws.