ComplyJet

WISP Template

A free, adaptable Written Information Security Program with sample clauses for ten sections, mapped to Massachusetts 201 CMR 17.00, the FTC Safeguards Rule (16 CFR 314), ISO 27001 and SOC 2.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with a real fact about your company. Delete any clause you cannot back with a real control, keep the numbering, and route the final version through your normal approval process, including review by counsel. Bracketed values are recommended defaults, not legal thresholds. No law or framework requires a document titled "WISP"; what the rules test is the content below. Write only what you actually do.

Company: [Company name]

Program Owner: [Role, e.g. Head of Engineering]

Version: [1.0]

Effective date: [Date]

Approved by: [Name, title]

Next review: [Date, at least annually]

Where each section comes from

WISP section	201 CMR 17.00	16 CFR 314.4	ISO 27001:2022	SOC 2 area
1. Purpose and scope	17.01, 17.03(1)	(b) scope	Clauses 4.3, 5.2	CC1
2. Program Owner	17.03(2)(a)	(a)	Clause 5.3	CC1, CC2
3. Risk assessment	17.03(2)(b)	(b)	Clause 6.1.2	CC3
4. Administrative safeguards	17.03(2)(c), (e)	(c)	Annex A 5.1, 6.1 to 6.7	CC5, CC6
5. Technical safeguards	17.04(1) to (7)	(c), (d)	Annex A 8.x	CC6, CC7
6. Physical safeguards	17.03(2)(g)	(c)	Annex A 7.x	CC6
7. Service providers	17.03(2)(f)	(f)	Annex A 5.19, 5.20	CC9
8. Training and discipline	17.03(2)(d), 17.04(8)	(e)	Annex A 6.3, 6.4	CC1, CC2
9. Incident response	17.03(2)(j)	(h), (j)	Annex A 5.24 to 5.28	CC7
10. Review and revision log	17.03(2)(h), (i)	(g), (i)	Clauses 9.2, 9.3, 10	CC4

The ISO 27001 and SOC 2 columns show the audit areas a section supports as evidence. Neither framework requires a WISP by name.

1. Purpose and scope

Clause 1.1 (17.03(1))

[Company] maintains this written information security program to protect personal information and other confidential data it holds, in paper and electronic form. It contains administrative, technical and physical safeguards appropriate to [Company]'s size, resources, the amount of data it stores and the sensitivity of that data.

Clause 1.2 Scope

This program applies to all employees, contractors, interns and any other person given access to [Company] systems or records, and to all systems, locations and records that hold personal information, including [list systems and office locations].

Clause 1.3 Related policies
This program points to: Information Security Policy, Access Control Policy, Data Encryption Policy, Physical Security Policy, Vendor Management Policy, Security Awareness Training Policy, Incident Response Plan, Risk Management Policy, Data Retention Policy.

2. Program Owner

Clause 2.1 (17.03(2)(a), 314.4(a))
The [Head of Engineering] is the Program Owner and is responsible for implementing and maintaining this program. The [VP of Operations] is the deputy. The Program Owner reports to the [CEO] in writing at least once a year on the state of the program, open risks and incidents.

3. Risk assessment

Clause 3.1 (17.03(2)(b), 314.4(b))
The Program Owner will assess reasonably foreseeable internal and external risks to the security, confidentiality and integrity of records containing personal information at least [annually] and whenever a material change occurs. The assessment is recorded in writing in the risk register below.

Asset	Threat	Existing safeguard	Decision and owner
[Customer database]	[Stolen credentials]	[MFA, least-privilege roles]	[Accept, review quarterly / owner]
[Laptops with exported files]	[Loss or theft]	[Full-disk encryption]	[ ]
[Shared drive with HR records]	[Over-broad access]	[Access reviews]	[ ]
[Payroll vendor]	[Vendor breach]	[Contract clause, annual review]	[ ]
[Paper onboarding forms]	[Left on desks]	[Locked cabinet]	[ ]

4. Administrative safeguards

Clause 4.1 Access (17.04(1), (2), 314.4(c))
Every person with access to [Company] systems receives a unique user ID. Multi-factor authentication is required for [all production, cloud and email systems]. Access to records containing personal information is limited to people who need it to do their job. Vendor-supplied default passwords are not permitted. User access is reviewed [quarterly].

Clause 4.2 Departures (17.03(2)(e))
Access to all systems and records is removed on the day a person leaves [Company] or changes role. HR notifies the Program Owner of every departure by [end of the last working day].

Clause 4.3 Records off premises (17.03(2)(c))
Records containing personal information may be taken or accessed outside [Company] premises only on approved devices over approved connections. Paper records may not be removed from the office unless the Program Owner has approved it. Lost or stolen devices and records must be reported to the Program Owner [within 24 hours].

5. Technical safeguards

Clause 5.1 Encryption (17.04(3), (5), 314.4(c))
Personal information is encrypted when transmitted across public networks or wirelessly, and when stored on laptops or other portable devices. [Company] [also encrypts personal information at rest in its production databases]. Company laptops use full-disk encryption and automatic screen lock. Personal information is not stored on personal devices or removable media unless the Program Owner has approved it.

Clause 5.2 Systems (17.04(4), (6), (7))
Systems holding personal information are monitored for unauthorized use or access. Internet-connected systems run up-to-date firewall protection and operating system security patches. Endpoints run up-to-date malware protection configured to receive current security updates. [Patches are applied within [30] days, critical patches within [7] days.]

Clause 5.3 Testing (314.4(d))
[Company] tests or monitors the effectiveness of its key controls [at least annually], including [vulnerability scanning and an annual penetration test], and records the results.

6. Physical safeguards

Clause 6.1 (17.03(2)(g))
Paper records containing personal information are kept in locked [cabinets or rooms] with access limited to [named roles]. Visitors are signed in and escorted. Paper and media are destroyed by [shredding or certified disposal] when no longer needed for business or legal reasons.

7. Service providers

Clause 7.1 (17.03(2)(f), 314.4(f))
Before a vendor receives personal information, the Program Owner will take reasonable steps to confirm the vendor can maintain appropriate safeguards. [Company] requires each such vendor, by written contract, to implement and maintain safeguards for that information. [Company] keeps the vendor list below and reviews it [annually].

Vendor	Data it can access	Contract safeguards clause	Last review
[Vendor]	[Data types]	[Yes / No, date]	[Date]
[Vendor]	[ ]	[ ]	[ ]

8. Training and discipline

Clause 8.1 (17.03(2)(d), 17.04(8), 314.4(e))
All personnel, including temporary and contract workers, complete security awareness training when they join and [annually] after that. Training covers this program, handling of personal information and how to report an incident. Violating this program may lead to disciplinary action, up to and including termination of employment or contract.

9. Incident response

Clause 9.1 (17.03(2)(j), 314.4(h))
Suspected incidents are reported to the Program Owner immediately. The Program Owner decides whether a breach of security has occurred, follows the [Incident Response Plan] and records the actions taken. After every incident, [Company] holds a post-incident review and documents any change made to its practices.

10. Review and revision log

Clause 10.1 (17.03(2)(h), (i), 314.4(g))
The Program Owner will review the scope of this program at least [annually] and whenever a material change in business practices may affect the security of personal information, including a new system, a new type of data, a new vendor or an incident. Each review and change is recorded in the revision log, and the [CEO] approves the updated version.

Version	Date	What changed	Approved by
[1.0]	[Date]	[Initial version]	[Name]
[ ]	[ ]	[ ]	[ ]

Acknowledgment

I have read and understand this written information security program and will follow it.

Name:	Signature:	Date:
[ ]	[ ]	[ ]

Evidence checklist

- Approved WISP with version and date
- Risk register with decisions and owners
- Signed acknowledgments from everyone in scope
- Training completion records
- Vendor list, contracts and reviews
- Incident log with post-incident reviews
- Annual review record and revision log

This template is general information, not legal advice. Have counsel review the final program, especially where state or sector rules apply. Free to use and adapt. Published by ComplyJet: complyjet.com/blog/wisp-template