CPF ORGANIZATIONAL CERTIFICATION AGREEMENT

PARTIES

This Organizational Certification Agreement ("Agreement") is entered into as of the ___ day of _____, 20___ ("Effective Date"), by and between:

[CERTIFICATION BODY NAME] ("Certification Body" or "CB")
A [jurisdiction] [entity type]
Authorized CPF Certification Body
Principal Office: [Address]
Email: [Email]

AND

[ORGANIZATION NAME] ("Organization" or "Certified Organization" upon certification)
A [jurisdiction] [entity type]
Registration Number: [Number]
Principal Office: [Address]
Email: [Email]

Collectively referred to as the "Parties" and individually as a "Party."

RECITALS

WHEREAS, Certification Body is authorized by CPF3 to operate the CPF Certification Scheme and certify organizations for psychological vulnerability management maturity;

WHEREAS, Organization desires to obtain organizational certification under the CPF Certification Scheme at one of four compliance levels (Level 1-4);

WHEREAS, Organization has implemented or is implementing the CPF methodology and CPF-27001:2025 requirements;

WHEREAS, Certification Body is willing to evaluate Organization's implementation and grant certification if requirements are met;

NOW, THEREFORE, in consideration of the mutual covenants and agreements contained herein, the Parties agree as follows:

1 DEFINITIONS

1.1 "Certification" means the formal attestation by Certification Body that Organization has achieved one of the following CPF Compliance Levels:

- Level 1: Foundation (CPF Score 100-149)
- Level 2: Intermediate (CPF Score 70-99)
- Level 3: Advanced (CPF Score 40-69)
- Level 4: Exemplary (CPF Score 0-39)

1.2 "CPF Score" means the aggregate vulnerability score (0-200 range) where lower scores indicate better security posture.

1.3 "Certification Scope" means the organizational units, locations, and personnel covered by certification, as detailed in Schedule A.

1.4 "CPF-27001:2025" means the CPF management system requirements standard.

1.5 "Surveillance Audit" means periodic audit to verify continued compliance.

1.6 "Nonconformity" means failure to meet a requirement.

2 CERTIFICATION SCOPE AND LEVEL

2.1 Certification Scope. The certification covers:

Legal Entity: _____

Business Units: _____

Locations: _____

Total Personnel in Scope: _____

Exclusions: _____

Detailed scope in Schedule A.

2.2 Target Certification Level:

☐ **Level 1: Foundation** (CPF Score 100-149)

☐ **Level 2: Intermediate** (CPF Score 70-99)

☐ **Level 3: Advanced** (CPF Score 40-69)

☐ **Level 4: Exemplary** (CPF Score 0-39)

3 CERTIFICATION PROCESS

3.1 Application Phase. Organization shall submit:

- Completed application form
- Valid CPF assessment report by certified Assessor/Auditor
- CPF policy approved by senior management
- Organizational chart showing CPF roles
- Privacy protection procedures
- Risk treatment plans for Red indicators
- Evidence of ISMS integration
- Management commitment letter
- Application fee payment

3.2 Application Review. Within 15 business days, Certification Body shall:

- Review completeness
- Verify CPF Score and assessment validity
- Review documentation for target level compliance
- Approve for audit or request additional information
- Assign qualified CPF Auditor

3.3 Certification Audit.

Stage 1 (Document Review, 1-3 days):

- Review CPF policy and procedures
- Assess readiness for Stage 2
- Identify gaps requiring correction

Stage 2 (Implementation Review, 3-10 days):

- Verification of CPF Score through sampling
- Review of methodology and privacy protections
- Verification of risk treatment
- Interviews with management and personnel
- Evidence review for target level requirements

- ISMS integration evaluation
- Effectiveness assessment

Audit Reporting (15 business days):

- Opening and closing meetings
- Written audit report
- Findings: Major NC, Minor NC, Observation, Opportunity

3.4 Corrective Actions. If nonconformities:

- Organization submits plan within 30 days
- Major NCs corrected before certification
- Minor NCs correctable within 90 days after
- Verification of effectiveness

3.5 Certification Decision. Within 15 business days:

- Grant at appropriate level
- Issue certificate and authorize Mark use
- Add to public registry
- Establish surveillance schedule
- Or deny with explanation and appeal rights

4 CERTIFICATION GRANT AND RIGHTS

4.1 Certification Grant:

- CPF Compliance Level certification
- Right to use Certification Mark
- Entry in public registry
- Certificate valid 3 years
- Access to resources

4.2 Use of Certification Mark:

- Website and marketing materials
- Proposals and presentations

- Office locations
- Email signatures
- Social media
- State: "CPF Certified Organization - Level [X]"

4.3 Restrictions:

- No modifications to Mark
- Not on products/services (applies to organization)
- Not for higher level than certified
- Not outside certification scope
- Not after expiration/suspension/revocation
- No transfer or sublicensing
- No misleading claims

5 OBLIGATIONS

5.1 Maintenance:

- Maintain systematic vulnerability management
- Continue CPF-27001:2025 implementation
- Maintain/improve CPF Score within level
- Update risk treatments
- Maintain privacy-preserving practices
- Provide adequate resources

5.2 Personnel:

- Maintain CPF Coordinator
- Level 2+: Minimum 1 certified Assessor
- Level 3+: Minimum 2 certified Assessors
- Level 4: Dedicated team with Auditor
- Ensure CPE maintenance
- Provide awareness training

5.3 Assessment and Monitoring:

- Level 1: Annual assessment
- Level 2: Quarterly cycles
- Level 3+: Continuous monitoring
- Use certified professionals
- Maintain documentation
- Track trends
- Report Red indicators per level requirements

5.4 Management Review:

- Level 1: Annual
- Level 2: Semi-annual
- Level 3+: Quarterly
- Document reviews with metrics, decisions, actions

5.5 Incident Reduction:

- Track human-factor incidents
- Establish baseline
- Level 2: 20% reduction
- Level 3: 40% reduction
- Level 4: 60% reduction
- Document evidence

5.6 Privacy and Ethics:

- Privacy protection framework
- Never use for individual profiling
- Minimum aggregation (10 individuals)
- Level 3+: Differential privacy ($\varepsilon \leq 0.1$)
- Time-delayed reporting (72 hours)
- Secure storage and transmission
- Level 3-4: Annual external privacy audit

5.7 Scope Changes. Notify within 30 days:

- Organizational changes

- Scope expansions/reductions
- Personnel changes (¿20%)
- CPF Coordinator changes
- Anything impacting certification

5.8 Cooperation:

- Grant access for surveillance
- Respond to inquiries timely
- Notify immediately of: breaches, score increases, complaints, legal actions, personnel loss
- Implement corrective actions

6 SURVEILLANCE

6.1 Requirements by Level:

Level 1:

- Annual surveillance by Assessor (1-2 days)
- Review program and results

Level 2:

- Bi-annual by Auditor (2-3 days)
- Quarterly desk review
- Verify incident reduction

Level 3:

- Annual by Auditor (3-5 days)
- Quarterly desk review of monitoring
- Annual privacy audit verification

Level 4:

- Annual by external Auditor (5-7 days)
- Monthly desk review
- Quarterly external privacy audit
- Bi-annual peer review

6.2 Process:

- 30 days advance notice
- Focus: Score trends, methodology, privacy, management review, incidents, changes
- Findings documented
- Corrective actions for NCs

6.3 Findings:

- No NCs: Continue
- Minor NCs: Plan within 30 days, implement within 90
- Major NCs: Immediate action, suspension if not corrected in 90 days

6.4 CPF Score Monitoring:

- Improvement: May apply for upgrade
- Degradation outside range: 90 days to restore or downgrade
- Score ¿149: Suspension pending corrective action

7 RECERTIFICATION

7.1 Requirement. Every 3 years.

7.2 Process:

- Notification 180 days before expiration
- Application 120 days before
- Full recertification audit
- Complete CPF Score assessment
- Review 3-year trends
- Continuous improvement evaluation
- Audit minimum 60 days before expiration
- Decision within 30 days
- New certificate with updated dates
- Level may change based on current score

7.3 Timing:

- Early: Up to 6 months before (new period from actual date)
- Late: Full re-certification as new applicant
- No grace period

8 FEES

8.1 Application Fee:

1-50 employees	$500
51-250	$1,000
251-1000	$1,500
1000+	$2,000

Non-refundable.

8.2 Audit Fees:

Size	Stage 1	Stage 2
1-50	$2,000	$4,000
51-250	$3,000	$7,000
251-1000	$5,000	$12,000
1000+	$8,000	$20,000

Complex/multi-site: Additional $1,500/day

8.3 Certification Fee:

1-50	$1,000
51-250	$2,000
251-1000	$3,500
1000+	$5,000

8.4 Annual Surveillance:

Level 1	30% of initial audit
Level 2	40% (bi-annual)
Level 3	50%
Level 4	60%

8.5 Recertification:

- Audit: 75% of initial
- Fee: Same as initial

8.6 Other:

- Scope expansion: $1,000-$5,000
- Follow-up for major NCs: $1,500/day
- Level upgrade: $2,000-$8,000
- Expedited: 25% surcharge
- Travel: Actual costs

8.7 Payment:

- Application: With submission

- Stage 1: Before audit
- Stage 2: Before audit
- Certification: Upon decision
- Surveillance: 30 days before
- All fees USD
- Late: 1.5% monthly interest
- Services suspended if ¿60 days overdue

9 SUSPENSION AND REVOCATION

9.1 Suspension Grounds:

- Score outside range
- Major NC not corrected (90 days)
- Failure to complete surveillance
- Failure to pay fees
- Privacy breach
- Key personnel loss
- Major organizational changes
- Mark misuse

9.2 Suspension Process:

- Written notice with grounds
- Immediate restriction on new Mark use
- Registry: "Suspended"
- Existing uses: Add "Certification Suspended"
- Max 180 days
- Remediation plan (30 days)
- Verification audit may be required
- Reinstatement upon remediation
- Revocation if not remediated

9.3 Revocation Grounds:

- Failure to remediate (180 days)
- Severe privacy violations
- Fraud/misrepresentation/falsification
- Systematic CPF-27001 violations
- Individual profiling
- Material breach
- Persistent Mark misuse
- Refusal to cooperate
- Insolvency/bankruptcy

9.4 Revocation Process:

- Written notice with grounds
- 30 days to respond
- Independent committee review
- Decision within 45 days
- If revoked: Immediate cessation, removal from registry, public notice, certificate return, no refunds, 2-year reapplication prohibition
- Right to appeal

9.5 Voluntary Withdrawal:

- 30 days notice
- Immediate cessation
- Certificate return
- No refunds
- May reapply anytime

10 APPEALS

10.1 Right to Appeal:

- Certification denial
- Level determination
- Suspension
- Revocation

- Downgrade
- Major NC disputes

10.2 Process:

- Written within 30 days
- Fee: $500
- Grounds and evidence
- Independent panel
- Decision within 45 days
- Options: Uphold/Modify/Reverse/Remand
- Fee refunded if successful
- Final and binding

11 CONFIDENTIALITY

11.1 CB Confidentiality:

- Maintain confidentiality of: Assessment data, scores, internal docs, business info, privacy methods, findings
- Limit access to audit team
- Not disclose except: Public registry info, to CPF3, to accreditation bodies, as required by law
- Personnel sign confidentiality agreements

11.2 Data Protection:

- Comply with GDPR/CCPA
- Implement security measures
- Process only for certification
- Notify breaches (24 hours)
- Cooperate in breach response

11.3 Retention:

- Records: 7 years after expiration/revocation
- Audit reports: 7 years
- Appeals/complaints: 10 years
- Secure destruction

12 LIMITATION OF LIABILITY

12.1 Disclaimer. NO WARRANTIES REGARDING BUSINESS OUTCOMES, INCIDENT PREVENTION, REGULATORY COMPLIANCE, OR INSURANCE IMPROVEMENTS.

12.2 Limitation. NO LIABILITY FOR INDIRECT, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES.

12.3 Cap. TOTAL LIABILITY NOT TO EXCEED FEES PAID IN 12 MONTHS PRECEDING CLAIM.

12.4 Exceptions: Gross negligence, confidentiality breaches, data protection violations, claims not permitted to limit by law.

13 INDEMNIFICATION

13.1 By Organization: From claims arising from Mark misuse, misrepresentation, privacy violations, false information, third-party claims.

13.2 By CB: From confidentiality breach, audit negligence, data violations.

14 GENERAL PROVISIONS

14.1 Governing Law. [Jurisdiction]

14.2 Disputes. Negotiation, mediation, then arbitration.

14.3 Entire Agreement. This Agreement and Schedules.

14.4 Amendment. CB may amend CPF-27001 (180 days notice).

14.5 Assignment. Organization cannot assign; CB may for business transfer.

14.6 Force Majeure. Neither liable for events beyond control.

14.7 Notices. Written to stated addresses.

14.8 Severability. Invalid provisions reformed.

14.9 Survival. Sections 10, 12, 13, 14 survive.

SIGNATURES

CERTIFICATION BODY:

By: _____ Date: _____

Name: _____ Title: _____

ORGANIZATION:

By: _____ Date: _____

Name: _____ Title: _____

SCHEDULE A: CERTIFICATION SCOPE

Legal Entity: _____

Business Units: _____

Locations: _____

Total Personnel: _____

Exclusions: _____

Justification: _____

Approved by:

CB: _____ Date: _____

Org: _____ Date: _____