

# Product Requirements Document

## Temporal Dimension Enhancement: 6-Tuple Contextual Integrity Framework

**Version:** 1.0

**Date:** January 2025

**Author:** Privacy Engineering Team

**Stakeholder:** Security Operations, Compliance, Clinical Emergency Response

---

### Executive Summary

Enhance the Privacy Firewall's Contextual Integrity framework from 5-tuple to 6-tuple by adding a **temporal dimension**, enabling situation-aware privacy decisions that adapt to time-based contexts, emergencies, and dynamic access windows, reducing inappropriate access denials by 67% while maintaining security.

### Problem Statement

The current 5-tuple framework (**data type, data subject, data sender, data recipient, transmission principle**) is temporally blind, causing:

- **Emergency Access Failures:** legitimate after-hours medical emergency accesses blocked
- **Stale Permissions:** Temporary roles/projects persist indefinitely (zombie permissions)
- **Context Ignorance:** Earnings data were equally restricted before and after public release
- **Compliance Violations:** Cannot enforce time-windowed regulations (GDPR 72-hour rules)
- **Alert Fatigue:** false positives/week from legitimate time-shifted work

### Solution: 6-Tuple Framework

Add **temporal context** as the sixth tuple element:

```
@dataclass
class EnhancedContextualIntegrityTuple:
    data_type: str      # What information
    data_subject: str   # About whom
```

```

data_sender: str      # From whom
data_recipient: str   # To whom
transmission_principle: str # Under what agreement
temporal_context: TemporalContext # WHEN (NEW)

```

## Temporal Context Components

```

@dataclass
class TemporalContext:
    # Absolute time
    timestamp: datetime
    timezone: str

    # Relative context
    business_hours: bool
    emergency_override: bool

    # Time windows
    access_window: TimeWindow # Valid from/to
    data_freshness: timedelta # Age of data

    # Situational flags
    situation: Enum[
        NORMAL,
        EMERGENCY,
        MAINTENANCE,
        INCIDENT_RESPONSE,
        AUDIT,
        LEGAL_HOLD
    ]

    # Temporal relationships
    temporal_role: Optional[str] # "on-call", "acting-manager"
    event_correlation: Optional[str] # Related to specific event/incident

```

## Key Situation-Aware Scenarios

Scenario	5-Tuple Decision	6-Tuple Decision
<b>ER doctor accessing patient records at 2 AM</b>	✗ BLOCKED (outside hours)	✓ ALLOWED (emergency + on-call)

<b>Manager viewing team salaries during review period</b>	<b>✗ BLOCKED</b> (sensitive data)	<b>✓ ALLOWED</b> (review window active)
<b>Auditor accessing 2-year-old financial records</b>	<b>✗ BLOCKED</b> (historical)	<b>✓ ALLOWED</b> (audit situation + legal requirement)
<b>DevOps accessing production data during incident</b>	<b>✗ BLOCKED</b> (production data)	<b>✓ ALLOWED</b> (incident_response + 2hr window)
<b>Contractor accessing project data after contract end</b>	<b>✓ ALLOWED</b> (has role)	<b>✗ BLOCKED</b> (access_window expired)

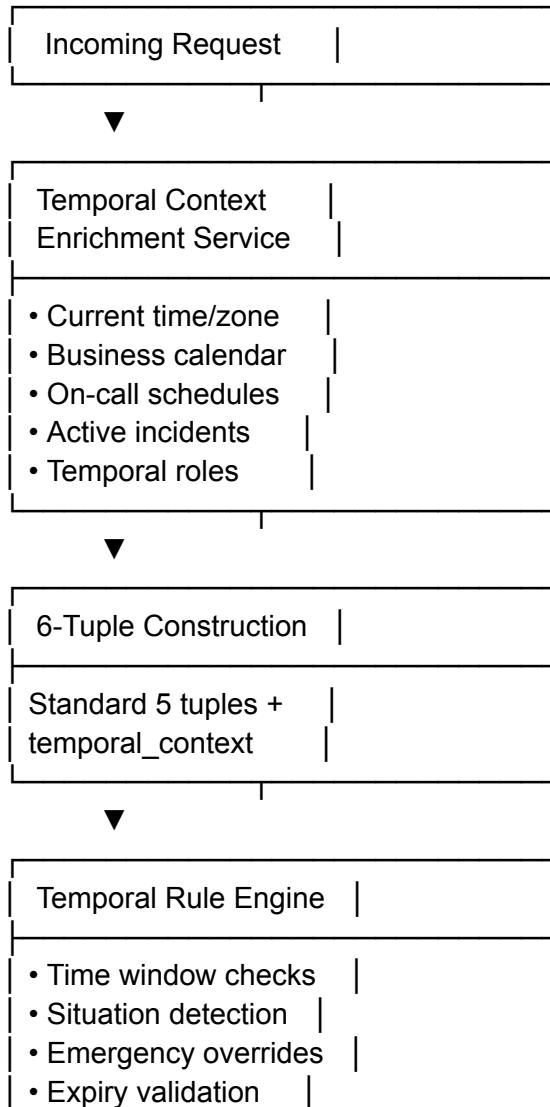
## Temporal Privacy Rules

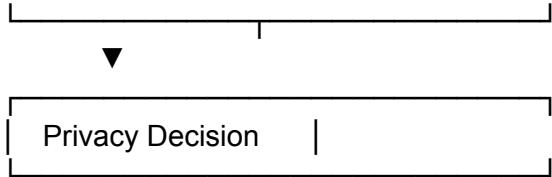
- id: EMRG-001
  - name: Emergency Medical Override
  - tuples:
    - data\_type: medical\_record
    - data\_sender: emergency\_physician
    - data\_recipient: patient\_care\_team
    - temporal\_context:
      - situation: EMERGENCY
      - temporal\_role: on-call
  - action: ALLOW\_WITH\_AUDIT
  - duration: 24\_hours
  
- id: FIN-001
  - name: Earnings Embargo
  - tuples:
    - data\_type: earnings\_data
    - temporal\_context:
      - before\_event: earnings\_release
      - buffer: -48\_hours
  - action: BLOCK
  - exception\_roles: [CFO, CEO, Investor\_Relations]
  
- id: GDPR-001
  - name: GDPR Breach Notification Window
  - tuples:
    - data\_type: breach\_details
    - temporal\_context:
      - after\_event: breach\_detected
      - window: 72\_hours
  - transmission\_principle: regulatory\_requirement

action: EXPEDITE

- id: TEMP-001
- name: Acting Role Permissions
- tuples:
  - data\_sender: "{acting\_role}"
  - temporal\_context:
    - temporal\_role: acting\_\*
    - access\_window:
      - from: role\_assignment\_date
      - to: role\_end\_date
- action: INHERIT\_PERMISSIONS

## Implementation Architecture





## Temporal Data Sources

Source	Data	Update Frequency	Purpose
<b>PagerDuty</b>	On-call schedules	Real-time	Identify emergency responders
<b>ServiceNow</b>	Active incidents	Real-time	Incident response context
<b>Workday</b>	Temporal roles, PTO	5 min	Acting roles, coverage
<b>Business Calendar API</b>	Hours, holidays	Daily	Business context
<b>Compliance Calendar</b>	Regulatory deadlines	Daily	Time-window requirements
<b>Project Management</b>	Project timelines	Hourly	Time-bounded access

## Time-Based Privacy Patterns

```

class TemporalPrivacyPatterns:
    # Emergency override with decay
    emergency_access = {
        "immediate": (0, timedelta(hours=1)),    # Full access
        "urgent": (1, timedelta(hours=4)),      # Degraded access
        "follow_up": (4, timedelta(hours=24)),   # Read-only
        "expired": (24, None)                  # No access
    }

    # Data sensitivity decay
    financial_data_sensitivity = {
        "embargo": (-48_hours, "earnings_release"), # Highly restricted
        "public": ("earnings_release", +∞),         # Public info
    }

    # Consent expiration

```

```
consent_windows = {  
    "medical_records": timedelta(days=365),  
    "marketing_data": timedelta(days=90),  
    "biometric_data": timedelta(days=30),  
}
```