# ReflectionLoop Implementation Guide

This comprehensive guide provides detailed instructions for implementing the ReflectionLoop PII/PHI detection and redaction tool in your organization. It covers everything from basic deployment to advanced customization and integration scenarios.

## Table of Contents

## Overview

ReflectionLoop is a single HTML file (136KB) that provides comprehensive PII/PHI detection and redaction capabilities. It requires no installation, runs completely offline, and works in any modern web browser.

### Key Components

- **Input Area**: Where users paste or upload text for analysis
- **Detection Engine**: 125+ regex patterns across 32 PII/PHI categories
- **Visual Review**: Color-coded highlighting with confidence scoring
- **Redaction System**: Click-to-exclude with [CATEGORY-REDACTED] replacements
- **Export Options**: Multiple formats including Word, PDF, CSV, and text

## Deployment Methods

### Option 1: Direct Distribution

1. Download `ReflectionLoop.html` from GitHub
2. Distribute via your preferred method:

- Email attachment

- Shared network drive

- Internal download portal

- USB drives for air-gapped environments

## Option 2: SharePoint/OneDrive Hosting

```powershell
# Upload to SharePoint document library
# Users can access directly or download local copies
# Enable versioning for updates
```

1. Upload to your SharePoint site

2. Set appropriate permissions

3. Share link with authorized users

4. Users can run directly from SharePoint or download

## Option 3: Microsoft Teams Integration

1. Upload to Teams Files tab

2. Pin for easy access

3. Team members can open directly in Teams

4. Works with Teams desktop and mobile apps

# Basic Usage

## Step-by-Step Workflow

1. **Open ReflectionLoop**
   - Double-click the HTML file, or
   - Access via your deployment method

2. **Input Text**
   - Paste text directly into input area
   - Upload .txt or .csv files
   - Support for up to 50,000 words

3. **Privacy Scan** (Button will pulse)
   - Click "Privacy Scan" to detect PII/PHI

- Processing shows progress bar
- Results appear with color-coded highlighting:
  - Red border = High confidence
  - Orange border = Medium confidence
  - Blue border = Low confidence

4. **Review Detections**
   - Hover over highlights to see confidence level
   - Click any highlight to exclude from redaction (turns gray)
   - Statistics update in real-time

5. **Clean Text** (Button will pulse after detection)
   - Click "Clean Text" to apply redactions
   - Original text replaced with [CATEGORY-REDACTED]
   - Excluded items remain unchanged

6. **Export Results**
   - "Copy Clean" - Copies to clipboard with formatting
   - "Export Report" - Choose format:
     - Word (.docx) - Preserves bold redactions
     - PDF - Opens print dialog
     - CSV - Detection details in spreadsheet
     - Text - Plain text with redactions

## Visual Workflow Indicators

The tool uses pulsing buttons to guide users:

- **Privacy Scan** pulses when text is entered
- **Clean Text** pulses after detection completes
- **Copy Clean** and **Clear All** pulse after cleaning

# Advanced Features

## Privacy Timer

- Activates after detection
- 5-minute countdown (visible in title bar)

- Auto-clears all data when expires

- Cannot be disabled (security feature)

### Inactive Session Blur

- Screen blurs after 45 seconds of inactivity

- Move mouse or touch screen to reactivate

- Provides visual privacy for unattended screens

- Works with privacy timer

### Confidence Scoring

The system assigns confidence based on contextual keywords:

```javascript
// High Confidence (2+ keywords present)
"My SSN is 123-45-6789" // Keywords: "my", "ssn"

// Medium Confidence (1 keyword)
"Contact: 555-123-4567" // Keyword: "contact"

// Low Confidence (pattern only)
"Reference 123-45-6789" // No keywords, pattern match only
```

### Detection Statistics

Real-time statistics display:

- Total detections

- Confidence breakdown (High/Medium/Low)

- Excluded count

- Items to be redacted

## Integration Scenarios

### Email Workflow Integration

For organizations using email for document sharing:

1. Create email template with ReflectionLoop attachment

2. Train users to run documents through tool before sending

3. Include in email security training

Example email template:

```
Subject: Document Sanitization Required

Please use the attached ReflectionLoop tool to remove any PII/PHI
before sharing documents externally.

Instructions:
1. Open the attached HTML file
2. Paste your document
3. Click "Privacy Scan"
4. Review and clean
5. Use the sanitized version

This is required for all external document sharing.
```

## Help Desk Integration

For IT support teams:

1. Add ReflectionLoop to technician toolkit

2. Require log sanitization before vendor escalation

3. Include in ticket handling procedures

```markdown
## Ticket Escalation Checklist
- [ ] Reproduce issue
- [ ] Gather logs
- [ ] Run logs through ReflectionLoop
- [ ] Attach sanitized logs to vendor ticket
- [ ] Note redaction report in ticket
```

## Development Environment Integration

For development teams:

```bash
# Add to your data preparation scripts
echo "Reminder: Sanitize production data with ReflectionLoop"
echo "Location: /tools/ReflectionLoop.html"
echo "Required for: test data, demo environments, training data"
```

## Compliance Workflow

For compliance teams:

1. Include in document review procedures

2. Generate redaction reports for audit trail

3. Use CSV export for compliance metrics

# Customization

## Adding Custom Detection Patterns

While the tool includes 125+ patterns, you can add organization-specific patterns:

```javascript
// Example: Add custom employee ID format
// Location: Inside detection_patterns object

custom_employee_id: {
    patterns: [
        /\b(?:ACME|CORP)-\d{6}-[A-Z]{2}\b/g,  // ACME-123456-US
    ],
    category: 'human_resources',
    type: 'Custom Employee ID',
    replacement: '[EMPLOYEE-ID-REDACTED]'
}
```

## Modifying Confidence Keywords

Add industry-specific keywords to improve accuracy:

```javascript
// Add to context_keywords object
custom_employee_id: ['acme', 'employee', 'staff', 'badge', 'id'],
```

## Adjusting Timer Settings

```javascript
// Change auto-clear timer (default: 300 seconds)
auto_clear_seconds: 600,  // 10 minutes

// Change inactivity blur (default: 45 seconds)
inactivityDelay: 60000,  // 60 seconds
```

## Custom Styling

The tool uses retro-style UI. To modernize:

```css
/* Add after existing styles */
.window {
    border-radius: 8px;
    box-shadow: 0 4px 12px rgba(0,0,0,0.1);
}

.button {
    border-radius: 4px;
    transition: all 0.2s;
}
```

# Security Considerations

## Network Isolation

The tool disables all network capabilities:

```javascript
// These APIs are disabled:
- fetch()
- XMLHttpRequest
- WebSocket
- EventSource
- sendBeacon
```

## Data Handling

- No data persistence (no localStorage/cookies)

- Memory-only processing

- Automatic cleanup after 5 minutes

- No telemetry or analytics

## Deployment Security

1. **Checksum Verification**

   ```bash
   # Generate checksum for integrity
   sha256sum ReflectionLoop.html
   ```

2. **Access Control**
   - Limit distribution to authorized users

   - Use your organization's access controls

   - Consider digitally signing the file

3. **Update Process**
   - Establish official distribution channel

   - Communicate updates via security bulletins

   - Maintain version control

# Performance Optimization

## Large Document Handling

For documents over 25,000 words:

1. **Split Processing**
   - Divide into logical sections

   - Process each section separately

   - Combine sanitized results

2. **Browser Settings**
   - Use Chrome/Edge for best performance

   - Close unnecessary tabs

   - Ensure adequate system memory

3. **Performance Indicators**

- Progress bar shows processing status

- Statistics update after completion

- Use "Copy Clean" for large documents (faster than export)

## Memory Management

The tool uses chunked processing:

- Default chunk size: 25,000 characters

- Helps to prevent browser freezing

- Allows processing of large documents

# Troubleshooting

## Common Issues

### Detection Not Working

- Verify text is in the input area

- Check browser console for errors (F12)

- Ensure JavaScript is enabled

- Try a different browser

### Export Not Working

- Check browser popup blocker for PDFs

- Ensure sufficient disk space

- Try a different export format

- Use "Copy Clean" as alternative

### Performance Issues

- Split large documents

- Close other browser tabs

- Check available system memory

- Use a modern browser version

### Copy/Paste Issues

- For Word: Use Ctrl+A, Ctrl+C in detection results

- For highlights: Chrome/Edge preserve formatting better

- Firefox: Bold works, highlights may not transfer

## Browser-Specific Notes

### Chrome/Edge

- Best performance and formatting preservation

- Highlights and bold transfer to Word

### Firefox

- Good performance

- Bold transfers, highlights may not

- Use markers for visual indication

**Note:** Only tested on Chrome, Edge, and Firefox. Other browsers may work but are not officially supported.

# Best Practices

## Organizational Implementation

1. **Training Program**
   - Include in security awareness training

   - Demonstrate during onboarding

   - Provide quick reference guide

   - Regular refreshers

2. **Policy Integration**
   - Add to data handling procedures

   - Require for external sharing

   - Include in compliance workflows

   - Document usage requirements

3. **Success Metrics**
   - Track adoption rates

   - Monitor redaction statistics

   - Measure security incidents

   - Calculate time savings

## User Guidelines

1. **Always Review Before Cleaning**
   - Check each detection
   - Understand what's being redacted
   - Exclude false positives
   - Verify completeness

2. **Document Verification**
   - Compare input/output word counts
   - Spot-check redactions
   - Ensure readability maintained
   - Verify required information remains

3. **Workflow Integration**
   - Make it routine, not exception
   - Build into existing processes
   - Share success stories
   - Provide feedback channel

## Security Awareness

Use ReflectionLoop as a training tool:

1. **Awareness Exercises**
   - Have users scan their emails
   - Review typical documents
   - Identify PII patterns
   - Discuss findings

2. **Measurable Improvement**
   - Pre/post training scans
   - Track PII reduction
   - Document behavior change
   - Celebrate improvements

# Need Help?

For questions or issues:

- Review the built-in Help documentation (Help button in tool)

- Check the README.md file

- Connect on <u>LinkedIn</u>

- Remember: This tool is provided as-is under MIT License

---

**Note**: This tool provides visual detection and redaction capabilities. Always verify results and maintain appropriate security controls for your organization's specific requirements.

*This is a personal hobby project, not associated or endorsed by any current or future employer.*