# FieldShield

*Targeted Data Security Functions*

# Protection Functions for Sensitive Files

- Field Level Encryption
- De-ID & Pseudonymization
- Data Masking & Redaction
- Compliance Audit Logging

**Product Summary**

IRI
The CoSort Company

## Why FieldShield?

Protecting sensitive information is a multi-faceted problem that requires data governance strategies and technologies that should follow the use of business data. Though many security solutions are available, the wrong design or execution choice can be inefficient, and leave data vulnerable to privacy breaches.

FieldShield™ is a faster, more effective way to protect sensitive data in files before they enter (or leave) a database or firewall. Data of this nature may include:

- **Personally identifiable information (PII)** which can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual
- **Protected health information (PHI)** which is any information in the medical record or designated record set that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a health care service
- **Payment card industry data (PCI)** which is used to process credit card payments, and is thus subject to fraud, hacking and other threats

FieldShield can privatize sensitive fields by encrypting, masking, or removing them according to your business rules.

## How Does FieldShield Work?

FieldShield allows you to define a specific protection method to each field in your files. With FieldShield, you can:

- Encrypt with a built in AES-256 library (or your own function)
- Filter input fields or redact records
- Mask by use of anonymization/obfuscation
- Mask by use of pseudonymization/de (and re)-identification
- Invoke custom protection methods

FieldShield uses the same data definition and manipulation language of the popular CoSort SortCL program to define your file layouts and protections. Each field name and attribute can be coupled with the same or different encryption library, masking method, de-identification code, pseudonymous lookup value, or custom security function that you write. The protection can even be conditioned upon specific attributes or ranges within the data.

FieldShield job scripts can be run on the command line, within batch and application programs, and eventually, from a Java GUI. You can specify the creation and location of an XML audit log with all job parameters and runtime details to record and prove the data protections you applied.

## What are the Advantages of FieldShield?

As a data protection tool, FieldShield offers:

- **Versatility** – secures sensitive data in files by applying a given protection function to one or more fields at a time
- **Efficiency** - field-only encryption is fast, and leaves remaining data open for processing
- **Flexibility** - specifies data protections on a conditional basis to better target a particular protection function based on a pattern, value, or range in a specific field or substring
- **Safety** - uses different security functions or encryption keys for each field
- **Simplicity** – one job script for multiple protections; one output for multiple recipients
- **Clarity** – uses self-documenting 4GL to define file layouts and field protections

## What are the Business Benefits of FieldShield?

- Protects data at its sources and endpoints
- Protected data can retain realism (for testing and sharing)
- Less cumbersome and more portable than DB column encryption
- Assigns protections appropriate to the data and its recipients
- Data stays safe even if it is stolen, or if a laptop is unencrypted
- Query-ready XML audit log helps verify compliance with data privacy regulations
- Simple job scripts save development and maintenance time

## What Applications are Compatible?

FieldShield runs on all Unix, Linux, and Windows platforms, and operates on file formats common to all of them, as well as mainframes. And, FieldShield uses the same metadata as:

- CoSort for data transformation and reporting
- RowGen for realistic test data generation
- NextForm for file and data type conversion
- Fast Extract (FACT) for Oracle and DB2

The data definition files are interchangeable among all IRI products, and are compatible with the Meta Integration Model Bridge (MIMB). MIMB's .ddf support means you can quickly convert file layouts in third-party ETL, BI, and modeling tools for use with FieldShield and other IRI software.

## Data & File Sources

- ASCII, EBCDIC and COBOL / Binary Datasets
- European, ISO, Japanese & U.S. Timestamps
- IP Addresses, Multi-Byte Chars, Whole Numbers
- DB2 & Oracle Tables - via IRI Fast Extract (FACT)
- ACUCOBOL-GT (Vision) Indexed Files
- LDIF (LDAP), Microsoft CSV, Flat XML
- Micro Focus Variable Length & I-SAM Files
- Sequential Flat Files (Line, Record, Variable)
- Unisys Variable Blocked Tape Format
- VSAM - via Clerity Mainframe Re-hosting
- W3C Common & Extended Log (Web)
- Other sources and targets via custom input or output procedures (use exits)

## Compatible Products

- CoSort - Data Transformation & Reporting
- FACT - Fast Extract for Oracle and DB2
- MIMB - Meta Integration Model Bridge
- NextForm - File and Data Type Conversion
- RapidACE - 3D Data Model Integration
- RowGen - Referentially Correct Test Data

## Supported Platforms

- UNIX (AIX, HP-UX, Solaris, Tru64 & more)
- Linux on x86 Itanium, IBM x/p/i/z; FreeBSD
- Windows (XP, 2000/2003/2008 Vista)

**FieldShield is currently available for script operations only.**

**A Java GUI is in development.**




**IRI, The CoSort Company**
2194 Highway A1A, Suite 303
Melbourne, FL 32937 USA

**1.321.777.8889**
**1.800.333.SORT**

**info@iri.com**
**www.iri.com**