Product Security White Paper

BD FACS™ Workflow Manager Software v1.0

BD is committed to providing secure products to our customers and recognizes the important benefits our products provide to patient health. We value the confidentiality, integrity and availability of all information, including protected health and personally identifiable information (e.g., PHI, PII and other types of personal data and sensitive data) and are committed to compliance with applicable regional, federal and local privacy and security laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) (EU) 2016/679.

BD has implemented reasonable administrative, technical and physical safeguards to help protect against security incidents and privacy breaches involving a BD product, provided those products are used in accordance with BD instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issue with product changes, technical bulletins and/or responsible disclosures to customers and regulators. BD continuously strives to improve security and privacy throughout the product lifecycle through:

- Privacy and Security by Design
- Product and Supplier Risk Assessment
- Vulnerability and Patch Management
- Secure Coding Practices and Analysis
- Vulnerability Scanning and Third-Party Testing
- Access Controls appropriate to Customer Data
- Incident Response
- Clear paths for two-way communication between customers and BD

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact the BD Product Security team:

Site: https://cybersecurity.bd.com/
Email: Cybersecurity@bd.com

Mail:

Becton, Dickinson and Company
Attn: Product Security
1 Becton Drive
Franklin Lakes, New Jersey 07417-1880

The purpose of this document is to detail how our security and privacy practices have been applied to the BD FACS™ Workflow Manager Software version 1.0, what you should know about maintaining security of this product, and how we can partner with you to ensure security throughout this product's lifecycle.

Contents

Product Description

As clinical laboratories strive for improved productivity, the need to interface laboratory instruments to a Laboratory Information System (LIS) or Hospital Information System (HIS) has become increasingly important. The BD FACS™ Workflow Manager solution provides a middleware and workflow optimization solution for clinical laboratories. The BD FACS™ Workflow Manager workstation is a small form factor Microsoft™ Windows™-based workstation that can be in the laboratory near the instruments it supports.

The BD FACS™ Workflow Manager allows for the direct transfer of information between several BD clinical instrument software applications and the customer's LIS. The software can be used to connect to the BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ instrument systems through the BD FACSuite™, BD FACSDuet™ and BD FACSVia™ Software applications.

Hardware Specifications

- HP™ Z2 Mini G5 (BD FACS™ Workflow Manager Host PC):
  - Intel™ Core™ i7- 10700 2.9GHz 8C 65W CPU
  - 16GB (1x16GB) DDR4 3200 SODIMM NECC Memory
  - Intel UHD Graphics 830 Core
  - Z Turbo Drive 1TB 2280 TLC Solid State Drive
  - 1Gb Intel Network Interface Connector
  - HP Z2 Mini Serial Port Adapter

Operating Systems

- Microsoft Windows 10 IoT Enterprise LTSC Build 1809, 64-bit

Third-Party Software

Vendor and Name	Version	Description
Active Directory Authentication Library for SQL	15.0.1300.359	Active Directory Authentication Library for SQL
Adobe™ Reader™ DC	19.012.20040	Adobe Reader DC
AvalonEdit	5.0.4	WPF-based text editor used in SharpDevelop
Bcrypt.Net-Next	3.1.3	A fixed, enhanced and namespace compatible version of BCrypt.Net port of jBCrypt implemented in C#.
BouncyCastle	1.8.5	The Bouncy Castle Crypto package is a C# implementation of cryptographic algorithms and protocols
Browser for SQL Server 2017	14.0.1000.169	Browser for SQL Server 2017

Vendor and Name	Version	Description
ByteSize	1.3.0	ByteSize is a utility class that makes byte size representation in code easier by removing ambiguity of the value being represented
Castle.Core	4.4.0	Castle Core, including DynamicProxy, Logging Abstractions and DictionaryAdapter
Castle.Windsor	4.1.1	Inversion of Control container
Castle.Windsor.MsDependencyInjection	3.3.1	Inversion of Control container
CefSharp.Wpf	65.0.1	The CefSharp Chromium-based browser component (WPF control)
ClosedXML	0.94.2	ClosedXML is a .NET library for reading, manipulating and writing Excel 2007+ (.xlsx, .xlsm) files
CommonServiceLocator	2.0.4	The library provides an abstraction over IoC containers and service locators
Cylance PROTECT	2.0.1570	Cyber threat prevention and remediation
Dapper	2.0.78	A high performance Micro-ORM supporting SQL Server, MySQL, Sqlite, SqlCE, Firebird etc..
DapperExtensions	1.6.3	A small library that complements Dapper by adding basic CRUD operations
Destructurama.Attributed	2.0.0	Use attributes to control how complex types are logged to Serilog
Expression.Blend.Sdk	1.0.2	Contains System.Windows.Interactivity for: - WPF 4.0, 4.5 -Silverligt 4.0, 5.0 - Windows Phone 7.1, 8.0 - Windows Store 8, 8.1
Extended.Wpf.Toolkit	3.5.0	Extended WPF Toolkit is a collection of WPF controls, components and utilities for creating next generation Windows applications
FakeItEasy	5.1.1	Mocking library for .NET, used in unit tests
Flee	1.2.2	Fast Lightweight Expression Evaluator, used in unit tests
FluentAssertions	5.6.0	A very extensive set of extension methods that allow you to more naturally specify the expected outcome of a TDD or BDD-style unit tests

Vendor and Name	Version	Description
FluentMigrator	3.1.3	FluentMigrator is a database migration framework for .NET
FluentMigrator.Runner	3.1.3	FluentMigrator is a database migration framework for .NET
FluentMigrator.Extensions.SqlServer	3.1.3	SQL Server extension for FluentMigrator
FluentMigrator.Tools	3.1.3	Tools for FluentMigrator
FluentValidation	8.4.0	A validation library for .NET that uses a fluent interface to construct strongly-typed validation rules
GemBox.Spreadsheet	43.0.0.1127	GemBox.Spreadsheet is a .NET component that enables developers to read, write, convert and print spreadsheet files.
gong-wpf-dragdrop	2.0.1	An easy to use drag'n'drop framework for WPF applications.
Halibut	4.1.0	Halibut is a secure, RPC-based communication framework.
Intel Network Connection Drivers	23.5	Intel Network Connection Drivers
Intel Graphics Drivers	25.20.100.6374	Intel Graphics Drivers
Intel Management Engine Components	1846.12.0.1177	Intel Management Engine Components
Mapster	3.3.2	A fast, fun and stimulating object to object mapper
Microsoft .Net	4.7	Microsoft .Net framework library
Microsoft Help Viewer	2.3.28107	Microsoft Help Viewer
Microsoft ODBC Driver 13 for SQL Server	14.0.1000.169	Microsoft ODBC Driver 13 for SQL Server
Microsoft ODBC Driver 17 for SQL Server	17.3.1.1	Microsoft ODBC Driver 17 for SQL Server
Microsoft OLE DB Driver for SQL Server	18.2.1.0	Microsoft OLE DB Driver for SQL Server

Vendor and Name	Version	Description
Microsoft SQL Server 2012 Native Client	11.4.7462.6	Microsoft SQL Server 2012 Native Client
Microsoft SQL Server 2017 (64-bit)	14.0.1000.169	Microsoft SQL Server 2017 (64-bit)
Microsoft SQL Server 2017 Setup (English)	14.0.1000.169	Microsoft SQL Server 2017 Setup (English)
Microsoft SQL Server 2017 T-SQL Language Service	14.0.1000.169	Microsoft SQL Server 2017 T-SQL Language Service
Microsoft Visual C++® 2013 Redistributable (x86)	12.0.30501.0	Microsoft Visual C++ 2013 Redistributable (x86)
Microsoft Visual C++® 2017 Redistributable (x64)	14.16.27029.1	Microsoft Visual C++ 2017 Redistributable (x64)
Microsoft Visual C++® 2017 Redistributable (x86)	14.16.27029.1	Microsoft Visual C++ 2017 Redistributable (x86)
Microsoft Visual Studio Tools for Applications 2017	15.0.27520	Microsoft Visual Studio Tools for Applications 2017
Microsoft VSS Writer for SQL Server 2017	14.0.1000.169	Microsoft VSS Writer for SQL Server 2017
Microsoft.AspNetCore	2.2.0	framework for building web apps and services with .NET and C#
Microsoft.AspNetCore.Authentication	2.2.0	ASP.NET Core common types used by the various authentication middleware components
Microsoft.AspNetCore.Authentication.JwtBearer	2.2.0	framework for building web apps and services with .NET and C#
Microsoft.AspNetCore.Mvc	2.2.0	ASP.NET Core middleware that enables an application to receive an OpenID Connect bearer token
Microsoft.AspNetCore.SignarlR	1.1.0	Components for providing real-time bi-directional communication across the Web
Microsoft.AspNetCore.WebUtilities	2.2.0	ASP.NET Core utilities, such as for working with forms, multipart messages, and query strings
Microsoft.CodeCom.Providers.DotNetCompilerPlatform	2.0.1	This provides support for new language features in systems using CodeDOM (e.g. ASP.NET runtime compilation) as well as improving the compilation performance of these systems

Vendor and Name	Version	Description
Microsoft.Extensions.DependencyInjection	2.2.0	Default implementation of dependency injection for Microsoft.Extensions.DependencyInjection
Microsoft.Extensions.PlatformAbstractions	1.1.0	Abstractions that unify behavior and API across .NET Framework, .NET Core and Mono
Microsoft.IdentityModel.Logging	5.4.0	Includes Event Source based logging support
Microsoft.IdentityModel.Tokens	5.4.0	Includes types that provide support for SecurityTokens, Cryptographic operations: Signing, Verifying Signatures, Encryption
Microsoft.Net.Compilers	3.1.0	.NET Compilers package
MvvmLight	5.4.1.1	The MVVM Light Toolkit is a set of components for the Model-View-ViewModel development pattern.
NETStandard.Library	2.0.3	A set of standard .NET APIs that are prescribed to be used and supported together
Newtonsoft.Json	12.0.2	Json.NET is a popular high-performance JSON framework for .NET
Nito.AsyncEx	4.0.1	A helper library for the Task-Based Asynchronous Pattern (TAP)
Realtek USB Ethernet Controller All-In-One Windows Driver	10.22.1212.2017	Realtek USB Ethernet Controller All-In-One Windows Driver
Serilog	2.8.0	Simple .NET logging with fully-structured events
Serilog.Extensions.Logging	2.0.4	Low-level Serilog provider for Microsoft.Extensions.Logging
Serilog.Extras.Attributed	2.0.0	Low-level Serilog provider for Microsoft.Extensions.Logging
Serilog.Settings.AppSettings	2.2.2	XML configuration (System.Configuration <appSettings>) support for Serilog
Serilog.Slinks.Console	3.1.1	A Serilog sink that writes log events to the console/terminal
Serilog.Slinks.EventLog	3.1.0	Serilog event sink that writes to the Windows event log
Serilog.Slinks.Literate	3.0.0	An alternative-colored console sink for Serilog that pretty-prints properties
Serilog.Slinks.MSSqlServer	5.1.2	A Serilog sink that writes events to Microsoft SQL Server

Vendor and Name	Version	Description
SimpleImpersonation	3.0.0	A tiny library that lets you impersonate any user, by acting as a managed wrapper for the LogonUser Win32 function
System.Composition	1.2.0	These packages provides a version of the Managed Extensibility Framework (MEF) that is lightweight and specifically optimized for high throughput scenarios, such as the web
System.IdentityModel.Tokens.Jwt	5.4.0	Includes types that provide support for creating, serializing and validating JSON Web Tokens
System.Reactive	4.1.5	Reactive Extensions (Rx) for .NET
System.Text.Encodings.Web	4.5.0	Provides types for encoding and escaping strings for use in JavaScript, HyperText Markup Language (HTML), and uniform resource locators (URL)
Topshelf	4.2.0	Topshelf is an open-source project for hosting services without friction.
Topshelf.Serilog	4.2.0	Topshelf is an open-source project for hosting services without friction.

Network Ports and Services

By default, the shipping configuration of the BD FACS™ Workflow Manager workstation operating system has the Microsoft Windows Firewall enabled, and the following ports are open.

1. Ports 5000-5002, 5101, 5200-5299, 10000-10099
2. Ports 123, 443, 445

We expect customers to configure the Windows Firewall if needed for their site networking specifications.

BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ Systems:

- Ports are customizable
- Customers can configure the specific ports that they use to connect with systems. In a default scenario, port 10000 is for connection to the customer's LIS server and ports in the range of 10001 to 10099 are used to connect to individual BD instrument systems in the customer lab. Please see the Data Flow diagram for an illustration.
- Port 123 is used to support the Simple Network Time Protocol (SNTP) if the workstations of the FACSDuet™, BD FACSLyric™ or BD FACSVia™ Systems are configured to synchronizes their clocks with the clock of the FWM workstation.
- Port 445 is used to support the SMB (Server Message Block) protocol for file transfer of report and data files from the BD FACSLyric™ System to the BD FACS™ Workflow Manager workstation.

For more details on how encryption is applied to network ports and services, see the section below on encryption.

Sensitive Data Transmitted

Data transmitted by BD FACS™ Workflow Manager Software to the customer LIS is encrypted as described below under the caption "Encryption". Customers sometimes include sensitive information depending on data sources other than BD clinical products:

- Personal Health Information (PHI), including:
  - Patient test results
- Patient identifying information (PII), including:
  - Common configurations include: First Name, Last Name, ID number, Date of Birth (DOB) and Gender
  - Additional fields can be configured by the customer, including Social Security Number (SSN) and Medical Records Number (MRN)

Sensitive Data Stored

Data stored by BD FACS™ Workflow Manager is encrypted as described below under the section "Encryption". Audit data may exist on the BD FACS™ Workflow Manager workstation until it is purged through an automated purge process configurable by the end user. Any information added by a user into a sample entry field may remain in the BD FACS™ Workflow Manager until the sample record is manually purged by the user. If a user enters personal health information or other sensitive information in those fields, that information may remain with the sample information until removed.

Users may use the BD FACS™ Workflow Manager to gather sensitive information from data sources other than BD clinical products. Such information could include:

- Personal Health Information, including:
  - Patient test results
- Patient identifying information (PII), including:
  - Common configurations include: First Name, Last Name, ID number, Date of Birth (DOB) and Gender
  - Additional fields can be configured by the customer, including Social Security Number (SSN) and Medical Records Number (MRN)

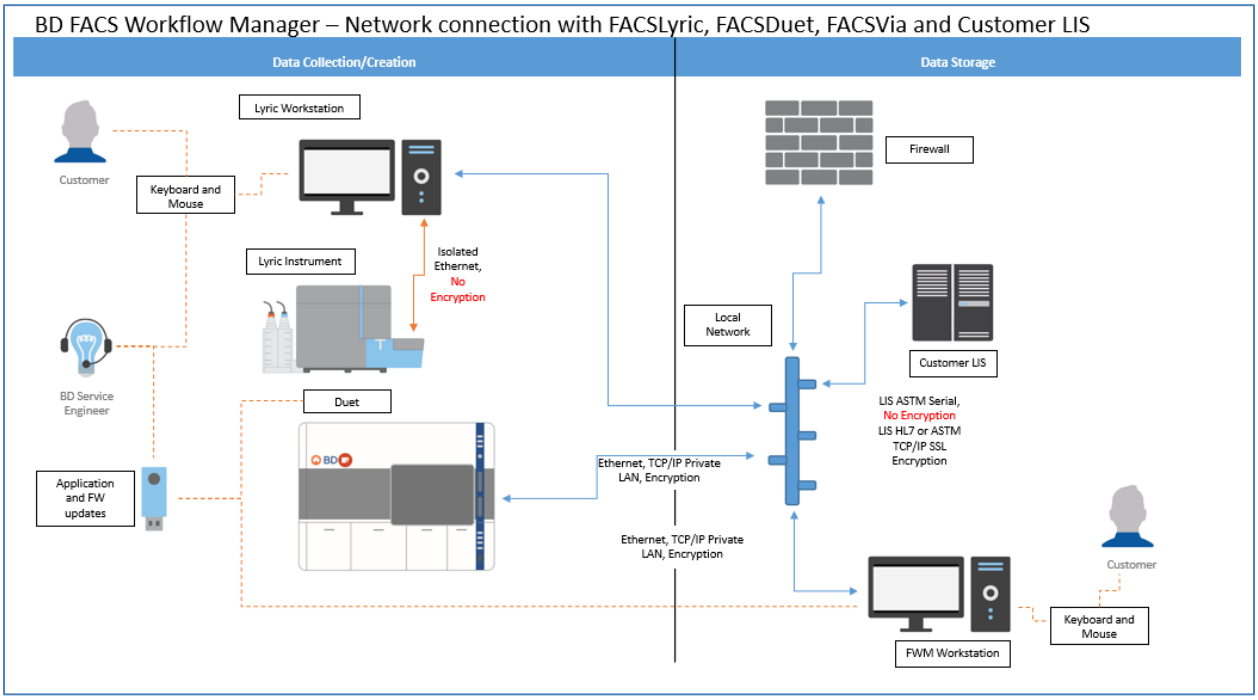
We recommend that users mitigate sensitive data handling through use of user-generated tracking numbers or local data identifiers not containing sensitive information and by not transmitting such information through BD FACS™ Workflow Manager Software.

Network and Data Flow Diagram

The BD FACS™ Workflow Manager option diagram below is an example of a typical laboratory network. The specific arrangement of each customer's network configuration will be

dependent on their network preferences and the number and type of instruments in the laboratory. The BD FACS™ Workflow Manager workstation is located in the customer lab in this illustration. The BD FACS™ Workflow Manager workstation can connect to multiple workstations; it is limited only by the number of licenses needed to connect both the customer's LIS and each instrument.

Remote desktop connection to the BD FACS™ Workflow Manager workstation is disabled in the operating system. However, the server comes with a keyboard, mouse and monitor for local maintenance.



BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ Systems:

Instrument workstations will publish patient results to the BD FACS™ Workflow Manager workstation, which will then send them to the LIS. The workstations can also pass data between each other so that they can synchronize work that must be done, for example, a sample preparation system (BD FACSDuet™) might pass the cytometer workstation (BD FACSLyric™) a worklist to run.

If the Document Management feature of BD FACS™ Workflow Manager is enabled, documents created on the BD FACSLyric™ System will be transferred to BD FACS™ Workflow Manager along with the results.

Malware Protection

The BD FACS™ Workflow Manager workstation comes installed with Windows Defender enabled and CylancePROTECT anti-malware pre-installed, however customers may install their preferred antivirus solution. It is the customer's responsibility to update Windows and the installed antivirus solution with the appropriate security patches and updates. See the document *Information security guidelines for BD Biosciences workstations* for additional information on configuring anti-malware.

Patch Management

BD FACS™ Workflow Manager application updates can be installed by the user or by BD Field Service during maintenance visits. Windows OS patches can be installed by the customer's IT system administrator after they have been reviewed and tested by BD. Patch bulletins are published approximately once per quarter to the BD.com website unless a critical vulnerability patch is released by Microsoft.

Authentication Authorization

The BD FACS™ Workflow Manager workstation comes with a default Windows administrator account and default password. We expect that the password for this account will be changed during installation per BD installation guidelines and managed by the customer. There is also a BD service account with a default password that BD FSEs can use for troubleshooting purposes.

Customers may manage workstation access simply through Windows OS user accounts and passwords for defined local administrative and operator profiles. Alternatively, customers can use Active Directory and user profiles with support from their local IT organization to manage user access.

Network Controls

Windows Firewall is enabled and configured to close unnecessary ports and general services that are not needed for system operation are disabled. We expect that customers may configure it to their site networking specifications during installation.

Additional information regarding use and configuration of anti-malware software, management of Windows user account settings, firewall settings and recommended usage of removable media is provided in the document *Information security guidelines for BD Biosciences workstations.*

BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ Systems:

The ports that BD FACS™ Workflow Manager Software is configured to communicate over (typically 10000-10099) must be left open, and the BD FACS™ Workflow Manager workstation should allow traffic coming from and going to IP addresses for the connected devices and systems in the lab. Whether those are a subnet or specific IP addresses depends solely on the customer network configuration.

Encryption

BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ Systems:

HTTPS encryption protocol using TLS 1.2 is supported through BD FACS™ Workflow Manager Software. For instructions on setting up your BD FACS™ Workflow Manager workstation ports to use HTTPS, please see the user guide.

LIS:
BD FACS™ Workflow Manager supports TLS encryption if communicating with the LIS over TCP. Encryption is not implemented for serial communication with the LIS.

BD FACS™ Workflow Manager:
The always Encrypted feature of Microsoft SQL Server is used to encrypt the BD FACS™ Workflow Manager database. Table columns containing Protected Health Information is encrypted.

Documents received from the BD FACSLyric™ System will be encrypted when stored on the file system of the BD FACS™ Workflow Manager workstation.

Audit Logging

- Application Auditing
  - Audit logs are stored in the BD FACS™ Workflow Manager database and can be accessed from the application
  - Auditable Events:
    - Service start/stop
    - User login/logout/failed login
    - Changes to library entities
    - Changes to settings
    - Viewing of patient/sample/result data
    - Creation/Modification/Deletion of patient/sample/result data by users or connection services (instruments / LIS)
  - Access to the audit log is limited to Administrators (Read and Export access)

Additional details on audit logging can be found in the BD FACS™ Workflow Manager User Guide.

Remote Connectivity

Remote connectivity to the BD FACS™ Workflow Manager workstation is disabled and there will be no access through Remote Desktop (RDP). A keyboard, mouse and monitor will be provided to connect to the BD FACS™ Workflow Manager workstation.

If a BD Assurity Linc™ Remote Support Software agent is installed on the system, remote access for troubleshooting might be requested by BD Service.

Windows OS-based remote access has been disabled as part of the OS hardening configuration. It can be enabled by the customer after installation is completed with guidance from a BD Field Service engineer. BD does not recommend use of Windows Remote Desktop due to known security vulnerabilities.

Service Handling

The BD FACS™ Workflow Manager Software will be updated following internal BD protocol for software releases. Additionally, BD will update any security sensitive patches on the instrument manager software and driver.

BD may perform routine service on the BD FACS™ Workflow Manager workstation dependent on the terms of a Service contract. BD will, however, not update the system with security patches during a service intervention. It is the responsibility of the customer to keep the workstation up to date on security patches, etc.

End-of-Life and End-of-Support

BD follows an internal process to provide end-of-life and end-of-support notifications directly to customers, where appropriate. At the time of this writing, there is no plan for end-of-life or end-of-support for this device and/or service.

Secure Coding Standards

No specific industry standard secure coding was used during development of the BD FACS™ Workflow Manager option however we conduct software source code vulnerability audits and perform monthly validation on operating system patches that address security issues.

System Hardening Standards

Windows Firewall is enabled on the workstation. Hardening standards have been applied to the workstation operating system in alignment with BD security requirements and a subset of DISA STIG guidelines. See the section on OS hardening in the *Information Security Guidelines* document for a complete list.

Risk Summary

- An application account with administrator privileges will be created for the customer during the installation of the BD FACS™ Workflow Manager. The account will have a minimum 8-character password. We expect that the customer will change the password of this account at first use and will configure accounts for their personnel limiting them to the following profiles:
    - Administrator: Users with this profile can perform all actions.
    - Operator: Users with this profile can view and manage the status of connections, review and manage requests and review results.
    - Reviewer: Users with this profile have the same access as Operators but can additionally approve and reject results.
    - Service: This profile is reserved for the BD Service account and cannot be assigned to any other account. With a BD Service account, patient details cannot be seen and actions in the requests and results module cannot be performed. BD Service account has no access to reporting workspace.

  - Super User: Users with this profile have the same access as Reviewer but additionally have access to manage the Library.

- Customers with administrative access can install third party software, which may introduce or expose vulnerabilities in the system.
  - Mitigation: Administrative access should be strictly controlled by the customer in collaboration with their local IT organization.

- There is the potential of PII transmission over a network if PII is being utilized as a parameter from the LIS. Default configuration of FACS™ Workflow Manager is HTTPS for instrument connectivity and TLS for TCP connectivity with the LIS.
  - Mitigation for BD FACSLyric™, BD FACSDuet™ and BD FACSVia™ Systems: We expect that the customer encrypts the traffic using HTTPS
  - Mitigation for LIS: We expect that the LIS encrypts the traffic using TLS

- There is the potential of PII being stored locally on the system if PII is being utilized as a parameter from the LIS.
  - Mitigation: Data is encrypted in transmission and at rest.

Manufacturer's Disclosure Statement for Medical Device Security

Otherwise known as the MDS2 form, this section provides an industry standard convention for security information.

MANUFACTURER DISCLOSURE STATEMENT FOR MEDICAL DEVICE SECURITY -- MDS2			
Manufacturer Name: Becton, Dickinson and Company, BD Biosciences	Device Model: FACS™ Workflow Manager	Document ID: #BD-10703	Document release date: 30 Apr 2021
	DEVICE DESCRIPTION		
Question ID	Question	Answer	Note #
DOC-1	Manufacturer Name	Becton Dickinson – Biosciences	
DOC-2	Device Description	LIS and Instrument Middleware solution	
DOC-3	Device Model	FACS™ Workflow Manager v1.0	
DOC-4	Document ID	#BD-10703	
DOC-5	Manufacturer Contact Information	Becton, Dickinson and Company BD Biosciences Attn: Product Security and Privacy 2350 Qume Dr. San Jose, CA 95131 For US support: 1-877-232-8995	
DOC-6	Intended use of device in network-connected environment:	The BD FACS™ Workflow Manager solution provides a middleware and workflow optimization solution for clinical laboratories.	
DOC-7	Document Release Date	2021-04-30	
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	See Notes	1
DOC-9	ISAO: Is the manufacturer part of an Information Sharing and Analysis Organization?	See Notes	1
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	See Notes	2
DOC-11	SaMD: Is the device Software as a Medical Device (i.e. software-only, no hardware)?	No	
DOC-11.1	Does the SaMD contain an operating system?	N/A	
DOC-11.2	Does the SaMD rely on an owner/operator provided operating system?	N/A	
DOC-11.3	Is the SaMD hosted by the manufacturer?	N/A	
DOC-11.4	Is the SaMD hosted by the customer?	N/A	
	DEVICE DESCRIPTION – NOTES		
Note 1	Coordinated vulnerability disclosure through the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Advisories and Reports Program and U.S. Food and Drug Administration, and National Health Information Sharing and Analysis Center (NH-ISAC)		
Note 2	Please refer to product security white paper for a basic diagram.		

	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION (MPII)	Yes, No, N/A or See Note	Note #
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (e.g. electronic Protected Health Information (ePHI))? If yes, provide details or reference in notes.	Yes	
MPII-2	Does the device maintain personally identifiable information?	Yes	
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	See Notes	1
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	No	
MPII-2.4	Does the device store personally identifiable information in a database? If yes, provide details or reference in notes.	Yes	
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	N/A	
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., a wearable monitoring device might export personally identifiable information to a server)?	See Notes	2
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	No	
MPII-2.8	Does the device allow the internal media to be removed by a service technician (e.g., for separate destruction or customer retention)?	Yes	
MPII-2.9	Does the device allow personally identifiable information records be stored in a separate location from the device's operating system (i.e. secondary internal drive, alternate drive partition, or remote storage location)?	Yes	
MPII-3	Does the device have mechanisms used for the transmitting, importing/exporting of personally identifiable information?	No	
MPII-3.1	Does the device display personally identifiable information (e.g., video display, etc.)?	Yes	
MPII-3.2	Does the device generate hardcopy reports or images containing personally identifiable information?	See Notes	2
MPII-3.3	Does the device retrieve personally identifiable information from or record personally identifiable information to removable media (e.g., removable-HDD, USB memory, DVD-R/RW,CD-R/RW, tape, CF/SD card, memory stick, etc.)?	No	
MPII-3.4	Does the device transmit/receive or import/export personally identifiable information via dedicated cable connection (e.g., RS-232, RS-423, USB, FireWire, etc.)?	Yes	
MPII-3.5	Does the device transmit/receive personally identifiable information via a wired network connection (e.g., RJ45, fiber optic, etc.)?	Yes	
MPII-3.6	Does the device transmit/receive personally identifiable information via a wireless network connection (e.g., WiFi, Bluetooth, NFC, infrared, cellular, etc.)?	No	
MPII-3.7	Does the device transmit/receive personally identifiable information over an external network (e.g., Internet)?	No	
MPII-3.8	Does the device import personally identifiable information via scanning a document?	No	

MPII-3.9	Does the device transmit/receive personally identifiable information via a proprietary protocol?	No	
MPII-3.10	Does the device use any other mechanism to transmit, import or export personally identifiable information? If yes, provide details or reference in notes.	No	
	MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION (MPII) – NOTES		
Note 1	Personally identifiable information is encrypted in database using SQL Server Always Encrypted.		
Note 2	Import/Export of personally identifiable information is done using X509 Certificate based encryption.		

	AUTOMATIC LOGOFF (ALOF)	Yes, No, N/A or See Note	Note #
	The device's ability to prevent access and misuse by unauthorized users if device is left idle for a period of time.		
ALOF-1	Can the device be configured to force reauthorization of logged-in user(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	Yes	
ALOF-2	Is the length of inactivity time before auto-logoff/screen lock user or administrator configurable?	Yes	
	AUTOMATIC LOGOFF (ALOF) – NOTES		

	AUDIT CONTROLS (AUDT)	Yes, No, N/A or See Note	Note #
	The ability to reliably audit activity on the device.		
AUDT-1	Can the medical device create additional audit logs or reports beyond standard operating system logs?	Yes	
AUDT-1.1	Does the audit log record a USER ID?	Yes	
AUDT-1.2	Does other personally identifiable information exist in the audit trail?	Yes	
AUDT-2	Are events recorded in an audit log? If yes, indicate which of the following events are recorded in the audit log:	Yes	
AUDT-2.1	Successful login/logout attempts?	Yes	
AUDT-2.2	Unsuccessful login/logout attempts?	Yes	
AUDT-2.3	Modification of user privileges?	Yes	
AUDT-2.4	Creation/modification/deletion of users?	Yes	
AUDT-2.5	Presentation of clinical or PII data (e.g. display, print)?	Yes	
AUDT-2.6	Creation/modification/deletion of data?	Yes	
AUDT-2.7	Import/export of data from removable media (e.g. USB drive, external hard drive, DVD)?	Yes	
AUDT-2.8	Receipt/transmission of data or commands over a network or point-to-point connection?	Yes	
AUDT-2.8.1	Remote or on-site support?	Yes	

	AUDIT CONTROLS (AUDT)	Yes, No, N/A or See Note	Note #
AUDT-2.8.2	Application Programming Interface (API) and similar activity?	Yes	
AUDT-2.9	Emergency access?	N/A	
AUDT-2.10	Other events (e.g., software updates)? If yes, provide details or reference in notes.	N/A	
AUDT-2.11	Is the audit capability documented in more detail? If yes, provide details or reference in notes.	Yes	
AUDT-3	Can the owner/operator define or select which events are recorded in the audit log? If yes, provide details or reference in notes.	No	
AUDT-4	Is a list of data attributes that are captured in the audit log for an event available? If yes, provide details or reference in notes.	Yes	
AUDT-4.1	Does the audit log record date/time?	Yes	
AUDT-4.1.1	Can date and time be synchronized by Network Time Protocol (NTP) or equivalent time source?	Yes	
AUDT-5	Can audit log content be exported?	Yes	
AUDT-5.1	Via physical media?	Yes	
AUDT-5.2	Via IHE Audit Trail and Node Authentication (ATNA) profile to SIEM?	No	
AUDT-5.3	Via Other communications (e.g., external service device, mobile applications)? If yes, provide details or reference in notes.	No	
AUDT-5.4	Are audit logs encrypted in transit or on storage media? If yes, provide details or reference in notes.	Yes	
AUDT-6	Can audit logs be monitored/reviewed by owner/operator? If no, provide details or reference in notes.	See Notes	1
AUDT-7	Are audit logs protected from modification? If yes, provide details or reference in notes.	Yes	
AUDT-7.1	Are audit logs protected from access? If yes, provide details or reference in notes.	Yes	
AUDT-8	Can audit logs be analyzed by the device? If so, provide reference in notes.	No	
	AUDIT CONTROLS (AUDT) – NOTES		
Note 1	Audit logs can only be viewed by users with administrator profile.		

	AUTHORIZATION (AUTH)	Yes, No, N/A or See Note	Note #
	The ability of the device to determine the authorization of users.		
AUTH-1	Does the device prevent access to unauthorized users through user login requirements or other mechanism?	Yes	
AUTH-1.1	Can the device be configured to use federated credentials management of users for authorization (e.g., LDAP, OAuth)? If yes, provide details or reference in notes.	See Notes	1
AUTH-1.2	Can the customer push group policies to the device (e.g., Active Directory)? If yes, provide details or reference in notes.	See Notes	2
AUTH-1.3	Are any special groups, organizational units, or group policies required? If yes, provide details or reference in notes.	No	
AUTH-2	Can users be assigned different privilege levels based on 'role' (e.g., user, administrator, and/or service, etc.)?	Yes	

AUTH-3	Can the device owner/operator grant themselves unrestricted administrative privileges (e.g., access operating system or application via local root or administrator account)?	Yes	
AUTH-4	Does the device authorize or control all API access requests? If no, provide details or reference in notes.	Yes	
AUTH-5	Does the device run in a restricted access mode, or 'kiosk mode', by default? If yes, provide details or reference in notes.	No	
	AUTHORIZATION (AUTH) - NOTES		
Note 1	Workstation access can be controlled through federated management. Application access is independent and does not support SSO.		
Note 2	Domain group policy can be applied to the workstation to manage compliance with customer IT security policies.		

	CYBER SECURITY PRODUCT UPGRADES (CSUP)	Yes, No, N/A or See Note	Note #
	The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade device's security patches.		
CSUP-1	Does the device contain any software or firmware which may require security updates during its operational life, either from the device manufacturer or from a third-party manufacturer of the software/firmware? If no, answer "N/A" to questions in this section.	Yes	
CSUP-2	Does the device contain an Operating System? If yes, complete 2.1-2.4.	Yes	
CSUP-2.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	No	
CSUP-2.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	
CSUP-2.3	Does the device have the capability to receive remote installation of patches or software updates?	See Notes	1
CSUP-2.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	See Notes	2
CSUP-3	Does the device contain Drivers and Firmware? If yes, complete 3.1-3.4.	Yes	
CSUP-3.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	3
CSUP-3.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	See Notes	3
CSUP-3.3	Does the device have the capability to receive remote installation of patches or software updates?	See Notes	1
CSUP-3.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes	
CSUP-4	Does the device contain Anti-Malware Software? If yes, complete 4.1-4.4.	Yes	
CSUP-4.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	Yes	
CSUP-4.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	
CSUP-4.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
CSUP-4.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes	

	CYBER SECURITY PRODUCT UPGRADES (CSUP)	Yes, No, N/A or See Note	Note #
CSUP-5	Does the device contain Non-Operating System commercial off-the-shelf components? If yes, complete 5.1-5.4.	Yes	
CSUP-5.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	See Notes	3
CSUP-5.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	No	
CSUP-5.3	Does the device have the capability to receive remote installation of patches or software updates?	Yes	
CSUP-5.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	Yes	
CSUP-6	Does the device contain other software components (e.g., asset management software, license management)? If yes, please provide details or reference in notes and complete 6.1-6.4.	No	
CSUP-6.1	Does the device documentation provide instructions for owner/operator installation of patches or software updates?	N/A	
CSUP-6.2	Does the device require vendor or vendor-authorized service to install patches or software updates?	N/A	
CSUP-6.3	Does the device have the capability to receive remote installation of patches or software updates?	N/A	
CSUP-6.4	Does the medical device manufacturer allow security updates from any third-party manufacturers (e.g., Microsoft) to be installed without approval from the manufacturer?	N/A	
CSUP-7	Does the manufacturer notify the customer when updates are approved for installation? If so, provide details or reference it in notes.	Yes	
CSUP-8	Does the device perform automatic installation of software updates?	No	
CSUP-9	Does the manufacturer have an approved list of third-party software that can be installed on the device? If so, describe or reference in notes the manufacturer-approved third-party software list and/or the manufacturing process for managing requests to approve additional third-party software.	No	
CSUP-10	Can the owner/operator install manufacturer-approved third-party software on the device themselves?	Yes	
CSUP-10.1	Does the system have mechanism in place to prevent installation of unapproved software?	See Notes	4
CSUP-11	Does the manufacturer have a process in place to assess device vulnerabilities and updates?	Yes	
CSUP-11.1	Does the manufacturer provide customers with review and approval status of updates?	No	
CSUP-11.2	Is there an update review cycle for the device? If so, provide details or reference it in notes.	See Notes	5
	CYBER SECURITY PRODUCT UPGRADES (CSUP) - NOTES		
Note 1	BD Assurity Linc™ Software can be installed for remote support. It is not pre-installed on the workstation.		
Note 2	Windows security patches can be applied to the workstation OS by local IT. BD posts security patch bulletins to its website to notify customers of recommended and not recommended patches.		
Note 3	Remote training may be provided through the remote support tool.		
Note 4	AppLocker is configured in the operating system to restrict installation and execution of unapproved applications.		
Note 5	Software components are reviewed for updates as part of the development process for new releases.		

	HEALTH DATA DE-IDENTIFICATION (DIDT)	Yes, No, N/A or See Note	Note #

	The ability of the device to directly remove information that allows identification of a person.		
DIDT-1	Does the device provide an integral capability to de-identify personally identifiable information? If yes, provide details or reference in notes.	Yes	
DIDT-1.1	Does the device support de-identification profiles that comply with the DICOM standard for de-identification? If so, provide details or reference in notes.	N/A	
	HEALTH DATA DE-IDENTIFICATION (DIDT) - NOTES		

	DATA BACKUP AND DISASTER RECOVERY (DTBK)	Yes, No, N/A or See Note	Note #
	The ability to recover after damage or destruction of device data, hardware, software, or site configuration information.		
DTBK-1	Does the device maintain long term primary storage of personally identifiable information / patient information (e.g. PACS)?	No	
DTBK-2	Does the device have a "factory reset" function to restore the original device settings as provided by the manufacturer?	No	
DTBK-3	Does the device have an integral data backup capability to removable media?	Yes	
DTBK-4	Does the device have an integral data backup capability to remote storage?	Yes	
DTBK-5	Does the device have a backup capability for system configuration information, patch restoration, and software restoration? If yes, provide details or reference in notes.	No	
DTBK-6	Does the device provide the capability to check the integrity and authenticity of a backup?	No	
	DATA BACKUP AND DISASTER RECOVERY (DTBK) – NOTES		

	EMERGENCY ACCESS (EMRG)	Yes, No, N/A or See Note	Note #
	The ability of the device user to access personally identifiable information in case of a medical emergency situation that requires immediate access to stored personally identifiable information.		
EMRG-1	Does the device incorporate an emergency access (i.e. "break-glass") feature? If yes, provide details or reference it in notes.	No	
	EMERGENCY ACCESS (EMRG) - NOTES		

	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)	Yes, No, N/A or See Note	Note #
	How the device ensures that the stored data on the device has not been altered or destroyed in a non-authorized manner and is from the originator.		

IGAU-1	Does the device provide data integrity checking mechanisms of stored health data (e.g., hash or digital signature)?	See Notes	1
IGAU-2	Does the device provide error/failure protection and recovery mechanisms for stored health data (e.g., RAID-5)?	No	
	HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU) - NOTES		
Note 1	Data is saved in ERP Format files which have an embedded checksum.		

	MALWARE DETECTION/PROTECTION (MLDP)	Yes, No, N/A or See Note	Note #
	The ability of the device to effectively prevent, detect and remove malicious software (malware).		
MLDP-1	Is the device capable of hosting executable software?	Yes	
MLDP-2	Does the device support the use of anti-malware software (or other anti-malware mechanism)? Provide details or reference in notes.	Yes	
MLDP-2.1	Does the device include anti-malware software by default?	Yes	
MLDP-2.2	Does the device have anti-malware software available as an option?	No	
MLDP-2.3	Does the device documentation allow the owner/operator to install or update anti-malware software? If yes, provide details or reference in notes.	See Notes	1
MLDP-2.4	Can the device owner/operator independently (re-)configure anti-malware settings?	Yes	
MLDP-2.5	Does notification of malware detection occur in the device user interface?	Yes	
MLDP-2.6	Can only manufacturer-authorized persons repair systems when malware has been detected? If yes, provide details or reference in notes.	See Notes	2
MLDP-2.7	Are malware notifications written to a log?	Yes	
MLDP-2.8	Are there any restrictions on anti-malware (e.g., purchase, installation, configuration, scheduling)?	See Notes	1
MLDP-3	If the answer to MLDP-2 is NO, and anti-malware cannot be installed on the device, are other compensating controls in place or available? If yes, provide details or reference in notes.	N/A	
MLDP-4	Does the device employ application whitelisting that restricts the software and services that are permitted to be run on the device? If yes, provide details or reference in notes.	See Notes	3
MLDP-5	Does the device employ a host-based intrusion detection/prevention system? If yes, provide details or reference in notes.	No	
MLDP-5.1	Can the host-based intrusion detection/prevention system be configured by the customer?	No	
MLDP-5.2	Can a host-based intrusion detection/prevention system be installed by the customer?	Yes	
	MALWARE DETECTION/PROTECTION (MLDP) - NOTES		
Note 1	Please refer to Information Security Guidelines for anti-malware configuration guidelines.		
Note 2	BD Service may need to reimage the workstation depending on the nature of the malware.		
Note 3	AppLocker is configured in the operating system to restrict installation and execution of unapproved applications.		

	NODE AUTHENTICATION (NAUT)	Yes, No, N/A or See Note	Note #
	The ability of the device to authenticate communication partners/nodes.		

NAUT-1	Does the device provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information (e.g. Web APIs, SMTP, SNMP)? If yes, provide details or reference in notes.	Yes	
NAUT-2	Are network access control mechanisms supported (E.g., does the device have an internal firewall, or use a network connection white list)? If yes, provide details or reference in notes.	Yes	
NAUT-2.1	Is the firewall ruleset documented and available for review? If yes, provide details or reference in notes.	Yes	
NAUT-3	Does the device use certificate-based network connection authentication?	Yes	
	NODE AUTHENTICATION (NAUT) - NOTES		

	CONNECTIVITY CAPABILITIES (CONN)	Yes, No, N/A or See Note	Note #
	All network and removable media connections must be considered in determining appropriate security controls. This section lists connectivity capabilities that may be present on the device.		
CONN-1	Does the device have hardware connectivity capabilities? If yes, provide details or a reference that identifies the hardware connectivity capabilities of the device. If no, indicate “none” in notes and answer “N/A” to questions in this section.	Yes	
CONN-1.1	Does the device support wireless connections?	No	
CONN-1.1.1	Does the device support Wi-Fi? If yes, please list or provide a reference to the Wi-Fi authentication protocols supported (e.g., WPA2 EAP-TLS) in the notes.	No	
CONN-1.1.2	Does the device support Bluetooth? If yes, please list or provide a reference to the Bluetooth security modes supported and indicate if they can be forced in the notes.	No	
CONN-1.1.3	Does the device support other wireless network connectivity (e.g. LTE, Zigbee, proprietary)? If yes, provide details or reference it in notes.	No	
CONN-1.1.4	Does the device support other wireless connections (e.g., custom RF controls, wireless detectors)? If yes, provide details or reference it in notes.	No	
CONN-1.2	Does the device support physical connections?	Yes	
CONN-1.2.1	Does the device have available RJ45 Ethernet ports?	Yes	
CONN-1.2.2	Does the device have available USB ports? If yes, provide details or reference that indicates use and how they are secured in notes.	Yes	
CONN-1.2.3	Does the device require, use, or support removable memory devices? If yes, provide details or reference it in notes.	Yes	
CONN-1.2.4	Does the device support other physical connectivity? If yes, provide details or reference it in notes.	See Notes	1
CONN-2	Does the manufacturer provide a list of network ports and protocols that are used or may be used on the device? If yes, provide details or reference it in notes.	Yes	
CONN-3	Can the device communicate with other systems within the customer environment? If yes, provide details or reference in notes.	Yes	

	CONNECTIVITY CAPABILITIES (CONN)	Yes, No, N/A or See Note	Note #
CONN-4	Can the device communicate with other systems external to the customer environment (e.g., a service host)? If yes, provide details or reference in notes.	No	
CONN-5	Does the device make or receive API calls? If yes, provide details or reference in notes.	See Notes	2
CONN-6	Does the device require an internet connection for its intended use? If yes, provide details or reference in notes.	No	
CONN-7	Does the device support Transport Layer Security (TLS)? If yes, provide details or reference about supported and prohibited versions of TLS in the notes.	See Notes	3
CONN-7.1	Is TLS configurable? If yes, provide details or reference in notes.	No	
CONN-8	Does the device provide operator control functionality from a separate device (e.g., telemedicine)? If yes, provide details or reference in notes.	No	
	CONNECTIVITY CAPABILITIES (CONN) - NOTES		
Note 1	RS-232 serial connection to LIS is supported.		
Note 2	Application receives Web API calls from connected instruments and client applications		
Note 3	TLS selection is managed by the OS. For LIS connections it can be forced in the settings to target the version of the .NET framework which supports TLS v1.2.		

	PERSON AUTHENTICATION (PAUT)	Yes, No, N/A or See Note	Note #
	The ability to configure the device to authenticate users.		
PAUT-1	Does the device support and enforce unique IDs and passwords for all users and roles (including service accounts)?	Yes	
PAUT-1.1	Does the device enforce authentication of unique IDs and passwords for all users and roles (including service accounts)? If no, provide details or reference in notes.	Yes	
PAUT-2	Is the device configurable to authenticate users through an external authentication service (e.g., MS Active Directory, NDS, LDAP, OAuth, etc.)? If yes, provide details or reference in notes.	No	
PAUT-3	Is the device configurable to lock out a user after a certain number of unsuccessful logon attempts? If yes, provide details or reference in notes.	See Notes	1
PAUT-4	Are all default accounts (e.g., technician service accounts, administrator accounts) listed in the documentation? If no, provide details or reference in notes.	Yes	
PAUT-5	Can all passwords be changed? If no, provide details or reference in notes.	Yes	
PAUT-6	Is the device configurable to enforce creation of user account passwords that meet established (organization specific) complexity rules? If so, provide details or reference in notes.	See Notes	2
PAUT-7	Does the device support account passwords that expire periodically? If yes, provide details or reference in notes.	See Notes	2
PAUT-8	Does the device support multi-factor authentication? If yes, provide details or reference in notes.	No	
PAUT-9	Does the device support single sign-on (SSO)? If yes, provide details or reference in notes.	No	
PAUT-10	Can user accounts be disabled/locked on the device?	Yes	
PAUT-11	Does the device support biometric controls?	No	

PAUT-12	Does the device support physical tokens (e.g. badge access)?	No	
PAUT-13	Does the device support group authentication (e.g. hospital teams)?	No	
PAUT-14	Does the application or device store or manage authentication credentials? If yes, provide details or reference in notes.	Yes	
PAUT-14.1	Are credentials stored using a secure method? If yes, provide details or reference in notes.	Yes	
	PERSON AUTHENTICATION (PAUT) - NOTES		
Note 1	Customer user accounts in the operating system are configured to lock out after five failed attempts.		
Note 2	User accounts in the workstation operating system can be configured for complexity and expiration.		

	PHYSICAL LOCKS (PLOK)	Yes, No, N/A or See Note	Note #
	Physical locks can prevent unauthorized users with physical access to the device from compromising the integrity and confidentiality of personally identifiable information stored on the device or on removable media		
PLOK-1	Is the device software only? If yes, answer "N/A" to remaining questions in this section.	No	
PLOK-2	Are all device components maintaining personally identifiable information (other than removable media) physically secure (i.e., cannot remove without tools)?	Yes	
PLOK-3	Are all device components maintaining personally identifiable information (other than removable media) physically secured behind an individually keyed locking device?	See Notes	1
PLOK-4	Does the device have an option for the customer to attach a physical lock to restrict access to removable media?	No	
	PHYSICAL LOCKS (PLOK) - NOTES		
Note 1	The Host PC device can be stored in a physically locked place or can be virtualized in a data center.		

	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)	Yes, No, N/A or See Note	Note #
	Manufacturer's plans for security support of third-party components within the device's life cycle.		
RDMP-1	Was a secure software development process, such as ISO/IEC 27034 or IEC 62304, followed during product development? If yes, provide details or reference in notes.	See Notes	1
RDMP-2	Does the manufacturer evaluate third-party applications and software components included in the device for secure development practices?	See Notes	2
RDMP-3	Does the manufacturer maintain a web page or other source of information on software support dates and updates? If yes, provide details or reference in notes.	No	
RDMP-4	Does the manufacturer have a plan for managing third-party component end-of-life? If yes, provide details or reference in notes.	See Notes	2
	ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP) - NOTES		
Note 1	BD software product development process is aligned with IEC 62304 and includes secure code analysis to identify findings based on industry standards such as OWASP and SANS.		
Note 2	Third-party components are reviewed for vulnerabilities and end-of-life with each release cycle. Findings are documented in the Product Security Management Plan for the product.		

	SOFTWARE BILL OF MATERIALS (SBoM)	Yes, No, N/A or See Note	Note #
	A Software Bill of Material (SBoM) lists all the software components that are incorporated into the device being described for the purpose of operational security planning by the healthcare delivery organization. This section supports controls in the RDMP section.		
SBOM-1	Is the SBoM for this product available? If yes, provide details or reference in notes.	Yes	
SBOM-2	Does the SBoM follow a standard or common method in describing software components? If yes, provide details or reference in notes.	Yes	
SBOM-2.1	Are the software components identified?	Yes	
SBOM-2.2	Are the developers/manufacturers of the software components identified?	Yes	
SBOM-2.3	Are the major version numbers of the software components identified?	Yes	
SBOM-2.4	Are any additional descriptive elements identified? If yes, provide details or reference in notes. [Guidance: Additional detail about descriptive elements (e.g., patch tags, software ID tags) are available in the following Standards and documents: ISO/IEC 19770-2:2015, Software Package Data Exchange (SPDX) 2.1]	No	
SBOM-3	Does the device include a command or process method available to generate a list of software components installed on the device? If yes, provide details or reference in notes.	No	
SBOM-4	Is there an update process for the SBoM? If yes, provide details or reference in notes.	See Notes	1
	SOFTWARE BILL OF MATERIALS (SBoM) – NOTES		
Note 1	Software components are reviewed for updates as part of the development process for new releases.		

	SYSTEM AND APPLICATION HARDENING (SAHD)	Yes, No, N/A or See Note	Note #
	The device's inherent resistance to cyber attacks and malware.		
SAHD-1	Is the device hardened in accordance with any industry standards? If yes, provide details or reference in notes.	See Notes	1
SAHD-2	Has the device received any cybersecurity certifications? If yes, provide details or reference in notes.	No	
SAHD-3	Does the device employ any mechanisms for software integrity checking	No	
SAHD-3.1	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the installed software is manufacturer-authorized?	No	
SAHD-3.2	Does the device employ any mechanism (e.g., release-specific hash key, checksums, digital signature, etc.) to ensure the software updates are the manufacturer-authorized updates?	No	
SAHD-4	Can the owner/operator perform software integrity checks (i.e., verify that the system has not been modified or tampered with)? If yes, provide details or reference in notes.	No	
SAHD-5	Is the system configurable to allow the implementation of file-level, patient level, or other types of access controls?	Yes	
SAHD-5.1	Does the device provide role-based access controls?	Yes	

	SYSTEM AND APPLICATION HARDENING (SAHD)	Yes, No, N/A or See Note	Note #
SAHD-6	Are any system or user accounts restricted or disabled by the manufacturer at system delivery? If yes, provide details or reference in notes.	Yes	
SAHD-6.1	Are any system or user accounts configurable by the end user after initial configuration?	Yes	
SAHD-6.2	Does this include restricting certain system or user accounts, such as service technicians, to least privileged access?	Yes	
SAHD-7	Are all shared resources (e.g., file shares) which are not required for the intended use of the device disabled? If yes, provide details or reference in notes.	Yes	
SAHD-8	Are all communication ports and protocols that are not required for the intended use of the device disabled? If yes, provide details or reference in notes.	Yes	
SAHD-9	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the intended use of the device deleted/disabled? If yes, provide details or reference in notes.	See Notes	1
SAHD-10	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the intended use of the device deleted/disabled? If yes, provide details or reference in notes.	See Notes	1
SAHD-11	Can the device prohibit boot from uncontrolled or removable media (i.e., a source other than an internal drive or memory component)? If yes, provide details or reference in notes.	See Notes	2
SAHD-12	Can unauthorized software or hardware be installed on the device without the use of physical tools? If yes, provide details or reference in notes.	See Notes	3
SAHD-13	Does the product documentation include information on operational network security scanning by users? If yes, provide details or reference in notes.	No	
SAHD-14	Can the device be hardened beyond the default provided state?	No	
SAHD-14.1	Are instructions available from vendor for increased hardening? If yes, provide details or reference in notes.	No	
SHAD-15	Can the system prevent access to BIOS or other bootloaders during boot?	See Notes	2
SAHD-16	Have additional hardening methods not included in 2.3.19 been used to harden the device? If yes, provide details or reference in notes.	No	
	SYSTEM AND APPLICATION HARDENING (SAHD) - NOTES		
Note 1	Windows operating system is hardened by application of DISA STIGs. Please refer to Information Security Guidelines for workstation operating system hardening specifications.		
Note 2	Workstation can boot from external media to allow BD Service restoration to factory default.		
Note 3	Customer is provided with local administrator account for system configuration and creation of additional user accounts. This account can install software and hardware so access to it should be restricted.		

	SECURITY GUIDANCE (SGUD)	Yes, No, N/A or See Note	Note #
	Availability of security guidance for operator and administrator of the device and manufacturer sales and service.		

SGUD-1	Does the device include security documentation for the owner/operator? If yes, provide details or reference in notes.	See Notes	1
SGUD-2	Does the device have the capability, and provide instructions, for the permanent deletion of data from the device or media? If yes, provide details or reference in notes.	No	
SGUD-3	Are all access accounts documented?	Yes	
SGUD-3.1	Can the owner/operator manage password control for all accounts?	Yes	
SGUD-4	Does the product include documentation on recommended compensating controls for the device?	See Notes	1
	SECURITY GUIDANCE (SGUD) – NOTES		
Note 1	Please refer to the Information Security Guidelines document additional security configuration information regarding the workstation and operating system.		

	HEALTH DATA STORAGE CONFIDENTIALITY (STCF)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure unauthorized access does not compromise the integrity and confidentiality of personally identifiable information stored on the device or removable media.		
STCF-1	Can the device encrypt data at rest? If yes, provide details or reference in notes.	See Notes	1
STCF-1.1	Is all data encrypted or otherwise protected? If yes, describe or provide a reference in notes.	See Notes	2
STCF-1.2	Is the data encryption capability configured by default?	See Notes	1,2
STCF-1.3	Are instructions available to the customer to configure encryption?	See Notes	1
STCF-2	Can the encryption keys be changed or configured? If yes, describe or provide a reference in notes.	See Notes	1
STCF-3	Is the data stored in a database located on the device? If yes, describe or provide a reference in notes.	See Notes	2
STCF-4	Is the data stored in a database external to the device? If yes, describe or provide a reference in notes.	No	
	HEALTH DATA STORAGE CONFIDENTIALITY (STCF) - NOTES		
Note 1	Data is encrypted at rest and in transfer. Data at rest is encrypted in the database and also on the file system. Additional disk encryption is not required. If the end-user wants to consider disk encryption, please refer to the BitLocker encryption topic in the Information Security Guidelines document for specific instructions.		
Note 2	All personally identifiable information is encrypted in the Workflow Manager database.		

	TRANSMISSION CONFIDENTIALITY (TXCF)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure the confidentiality of transmitted personally identifiable information.		
TXCF-1	Can personally identifiable information be transmitted only via a point-to-point dedicated cable?	No	

TXCF-2	Is personally identifiable information encrypted prior to transmission via a network or removable media? If yes, describe or provide a reference in notes.	See Notes	1,2
TXCF-2.1	If data is not encrypted by default, can the customer configure encryption options?	Yes	
TXCF-3	Is personally identifiable information transmission restricted to a fixed list of network destinations?	Yes	
TXCF-4	Are connections limited to authenticated systems? If yes, describe or provide a reference in notes.	See Notes	1,2
TXCF-5	Are secure transmission methods supported/implemented (DICOM, HL7, IEEE 11073)? If yes, describe or provide a reference in notes.	Yes	
	TRANSMISSION CONFIDENTIALITY (TXCF) - NOTES		
Note 1	The system is using by default x509 certificate-based HTTPS for communication between FWM connections and FWM clients. Connected FACSLyric™ and FACSDuet™ instruments can be configured to use x509 certificate-based HTTPS encryption.		
Note 2	The system can be configured to use x509 certificate-based TLS encryption. The system has an option to choose the encryption or let the OS handle the encryption protocol.		

	TRANSMISSION INTEGRITY (TXIG)	Yes, No, N/A or See Note	Note #
	The ability of the device to ensure the integrity of transmitted data.		
TXIG-1	Does the device support any mechanism (e.g., digital signatures) intended to ensure data is not modified during transmission? If yes, describe or provide a reference in notes.	See Note	1,2
TXIG-2	Does the device include multiple sub-components connected by external cables? If yes, describe or provide a reference in notes.	No	
	TRANSMISSION INTEGRITY (TXIG) - NOTES		
Note 1	The system is using by default x509 certificate-based HTTPS for communication between FWM connections and FWM clients. Connected FACSLyric™ and FACSDuet™ instruments can be configured to use x509 certificate-based HTTPS encryption.		
Note 2	The system can be configured to use x509 certificate-based TLS encryption for LIS connections using the TCP/IP protocol. The system has an option to force the encryption type or let the OS handle the encryption type.		

	REMOTE SERVICE (RMOT)	Yes, No, N/A or See Note	Note #
	Remote service refers to all kinds of device maintenance activities performed by a service person via network or other remote connection.		
RMOT-1	Does the device permit remote service connections for device analysis or repair? If yes, describe or provide a reference in notes.	Yes	
RMOT-1.1	Does the device allow the owner/operator to initiative remote service sessions for device analysis or repair?	Yes	
RMOT-1.2	Is there an indicator for an enabled and active remote session?	Yes	
RMOT-1.3	Can patient data be accessed or viewed from the device during the remote session?	See Notes	1
RMOT-2	Does the device permit or use remote service connections for predictive maintenance data? If yes, describe or provide a reference in notes.	See Notes	2

	REMOTE SERVICE (RMOT)	Yes, No, N/A or See Note	Note #
RMOT-3	Does the device have any other remotely accessible functionality (e.g. software updates, remote training)? If yes, describe or provide a reference in notes.	See Notes	3
	REMOTE SERVICE (RMOT) - NOTES		
Note 1	Support engineers access the device using the service built in account, the service account does not expose personally identifiable information.		
Note 2	Instrument operation log files and Windows OS data from the workstation may be transferred during a remote support session.		
Note 3	Remote training may be provided through the remote support tool.		

	OTHER SECURITY CONSIDERATIONS (OTHR)
	NONE

Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and BD, or BD's subsidiaries or affiliates (collectively, "BD"). BD does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper, and customer agrees to indemnify and hold BD harmless from the same.

The BD FACSDuet™ Sample Preparation System and BD flow cytometers are Class 1 Laser Products.

The BD FACSVia™ System, BD FACSDuet™ Sample Preparation System and the BD FACSLyric™ Flow Cytometer with the BD FACSuite™ Clinical and BD FACSuite™ Applications are CE marked in compliance with the European In Vitro Diagnostic Medical Device Directive 98/79/EC.

The BD FACSVia™ System is discontinued.

CE