ISOLOCITY SOFTWARE VALIDATION

EudraLex The Rules Governing Medicinal Products in the European Union
Volume 4 - Good Manufacturing Practice Medicinal Products for Human and Veterinary
Use Annex 11: Computerised Systems

Legal basis for publishing the detailed guidelines: Article 47 of Directive 2001/83/EC on the Community code relating to medicinal products for human use and Article 51 of Directive 2001/82/EC on the Community code relating to veterinary medicinal products. This document provides guidance for the interpretation of the principles and guidelines of good manufacturing practice (GMP) for medicinal products as laid down in Directive 2003/94/EC for medicinal products for human use and Directive 91/412/EEC for veterinary use.

Status of the document: revision 2

Reasons for changes: The Annex has been revised in response to the increased use of computerised systems and the increased complexity of these systems. Consequential amendments are also proposed for Chapter 4 of the GMP Guide.

Deadline for coming into operation: 30 June 2011

Principle

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

The application should be validated; IT infrastructure should be qualified.

Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance. There should be no increase in the overall risk of the process.

General

1. **Risk Management**

Risk management should be applied throughout the lifecycle of the computerised system considering patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

The table below identifies any probable risks that may impact the success of the V&V (Verification & Validation) program.

Risk Type	Details	Risk Rating	Contingency
Human Error	QA misses' system error that required manual check	Medium	Second QA Checker & Automated Test Suite
Subsequent bugs	New builds may inadvertently create errors in other modules	High	Ensure system is updated with all test cases for test suite and releases are QA by internal staff and independent contractor.

2. Personnel

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons, and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

Role	Name	Responsibility
Operations Manager	Emily Soares	Development including enhancements and maintenance, and Customer Success
Director of Digital Marketing	Mukut Chakraborty	Marketing efforts including updates to clients on system releases
Director of Sales	Chris Budd	Sales efforts including illustrating software features and launches to prospective clients. Internal Subject matter expert.
Software Developer	Cristian Aldana	Build software enhancements based on specifications and fix bugs

Software Developer	Evan Al Diab	Build software enhancements based on specifications and fix bugs
Software Developer	Sinem Oyan	Build software enhancements based on specifications and fix bugs
Software Developer	Archana Korat	Build software enhancements based on specifications and fix bugs
Quality Assurance	Mehedi Hassan	Run Test Suite and manually QA software for each release and hotfix (including regression testing). Updates validation documentation and completes performance and operational qualification for all releases. Documents the results of the validation.

Identify the software tools, techniques, and methodologies to be used by the verification and validation team.

Tool	Purpose	Details
Selenium Test Suite	Automatic QA of entire software each time code is added/altered	Run by QA and overseen by Operations. Once all test cases have been reviewed by test suite, errors found must be reviewed by Operations and resolved by the Senior Software Engineer
Manual Regression Testing	Review of software to ensure the system is working as expected and has not produced unintended outcomes in the code	Performed each quarter by QA
Validation Plan	Lists all the test plans for each module step-by-step to emphasize what is expected from the software	Update and modify validation plan as new modules are changed/added

3. Suppliers and Service Providers

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the

manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

Isolocity terms and conditions https://isolocity.com/software-terms-and-conditions/

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

Quality and Compliance complete regular reviews of Isolocity. The next review is scheduled for 2023. https://www.qualityandcompliance.com/

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

AWS Agreements and security protocols can be provided upon request. Isolocity is hosted with AWS, see https://aws.amazon.com/artifact/ for all available artifacts.

Project Phase

4. Validation

4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.

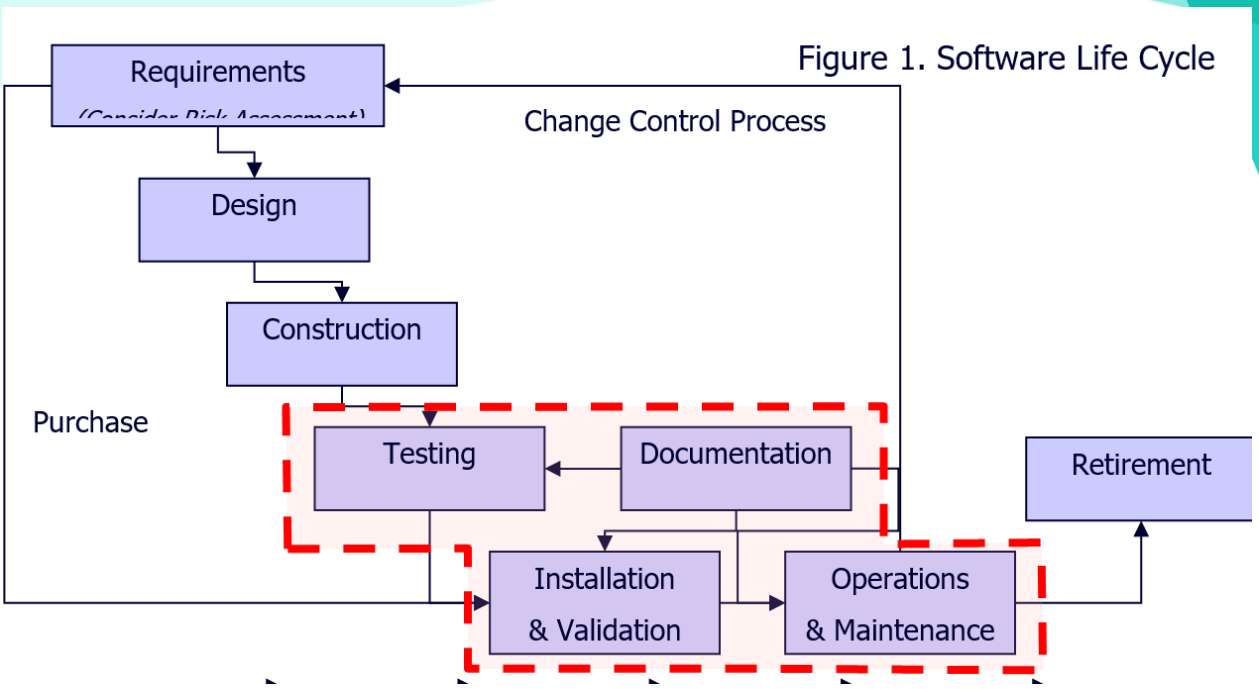


Figure 1. Software Life Cycle

4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.

All testing and validation steps follow these steps:

Requirements Phase and System Acceptance Test Specification

This phase identifies, specifies, analyzes, and documents all the requirements that the software must satisfy regarding functionality, performance, design constraints, attributes, and external interfaces. It is important to perform a risk assessment during this phase.

Design Phase

This phase develops, documents, and reviews a design that satisfies the requirements previously documented.

Answers to some key questions should be documented during formal design reviews. These include:

· Have the appropriate tasks and expected results, outputs, or products been established for each software life cycle activity?

· Do the tasks and expected results, outputs, or products of each software life cycle activity:

Comply with the requirements of other software life cycle activities in terms of correctness, completeness, consistency, and accuracy?

Satisfy the standards, practices, and conventions of that activity?

Establish a proper basis for initiating tasks for the next software life cycle activity?

Construction Phase

This phase takes each element documented in the design phase and translates it into a programming language. This phase is often known as a "coding" or "build" phase.

Testing Phase

This phase runs the software through test cases and analyzes any failure to determine which phase contributed to such error.

Installation and Validation Phase

This phase executes tests for the installation and integration of the software into the equipment (i.e., other software, data, hardware), and the documentation of the approval of the software for operational use. User site testing is a very important practice to consider because it helps eliminate errors (i.e., bugs) that may arise after the software is installed on different equipment. https://docs.google.com/spreadsheets/d/15BUsOaqINAJRlboLUt5Z3cFxua6rWTbApfbnbj7iX10/edit#gid=1494046008 (file associated with this procedure) must be used to ensure complete assessment of all aspects of the software (especially ensuring that calculation functions are not the only item assessed) and to begin the documentation.

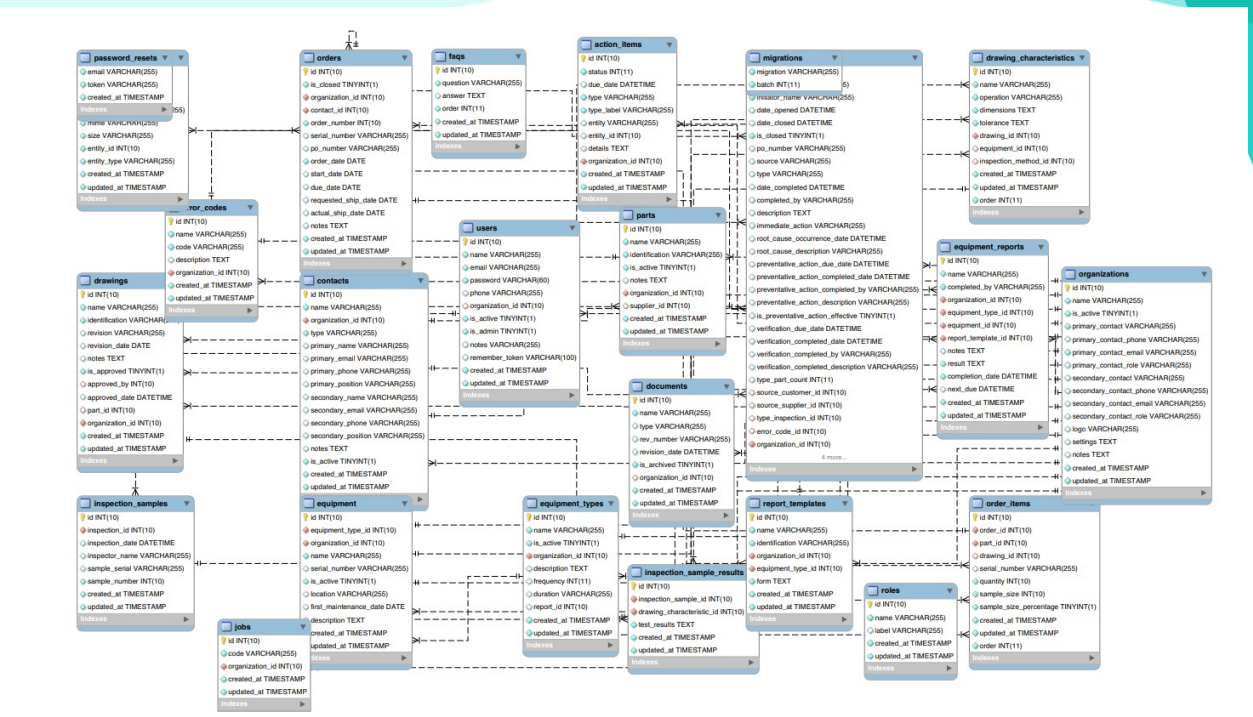
Documentation Phase

This phase handles the technical documentation of all the phases described above. Evidence must be retained in association with the methods used.

Operations and Maintenance

Once the software has been approved for operational use, routine maintenance may be performed to remove errors, to respond to new or modified equipment, or to adapt the software to changes in the operating environment. All planned changes must be approved by the Director of Operations before work is started. After any modifications, software must be verified and validated again.

4.3 An up-to-date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software prerequisites, and security measures should be available.



4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life cycle.

Client Related Process.

https://isolocity.com/knowledge-base/

4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.

Client related process

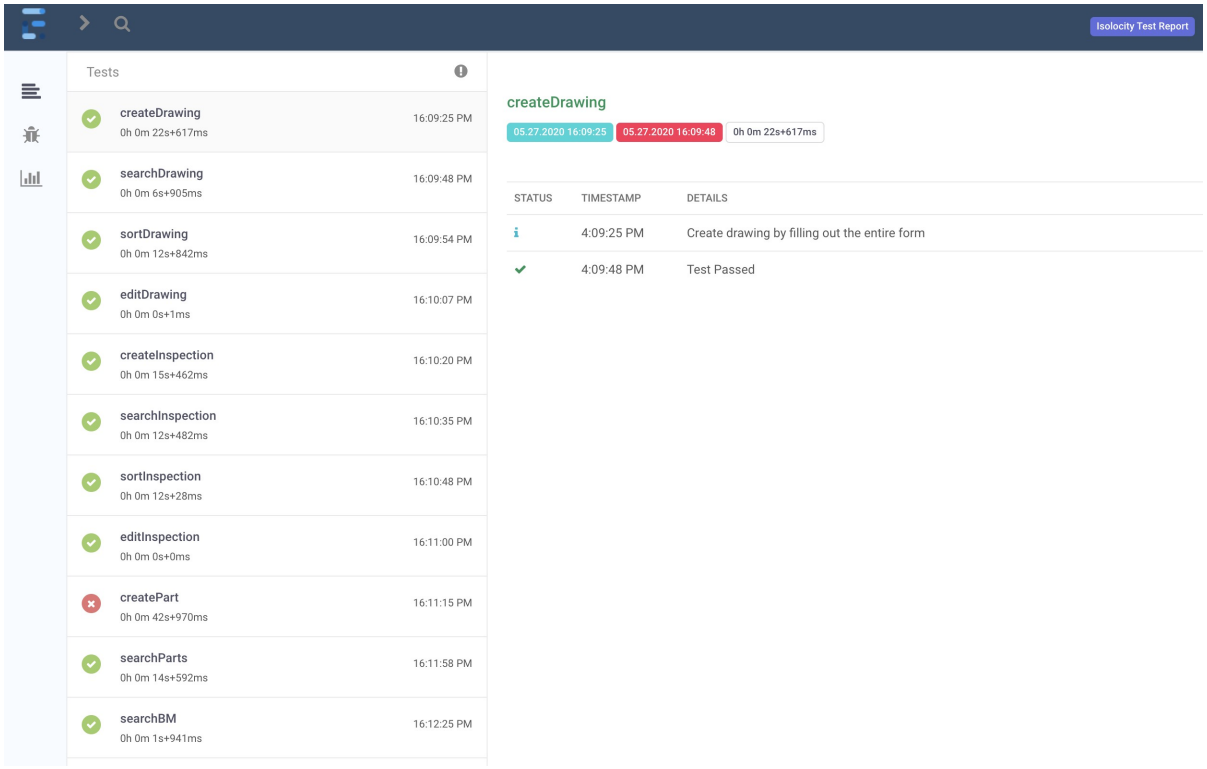
4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.

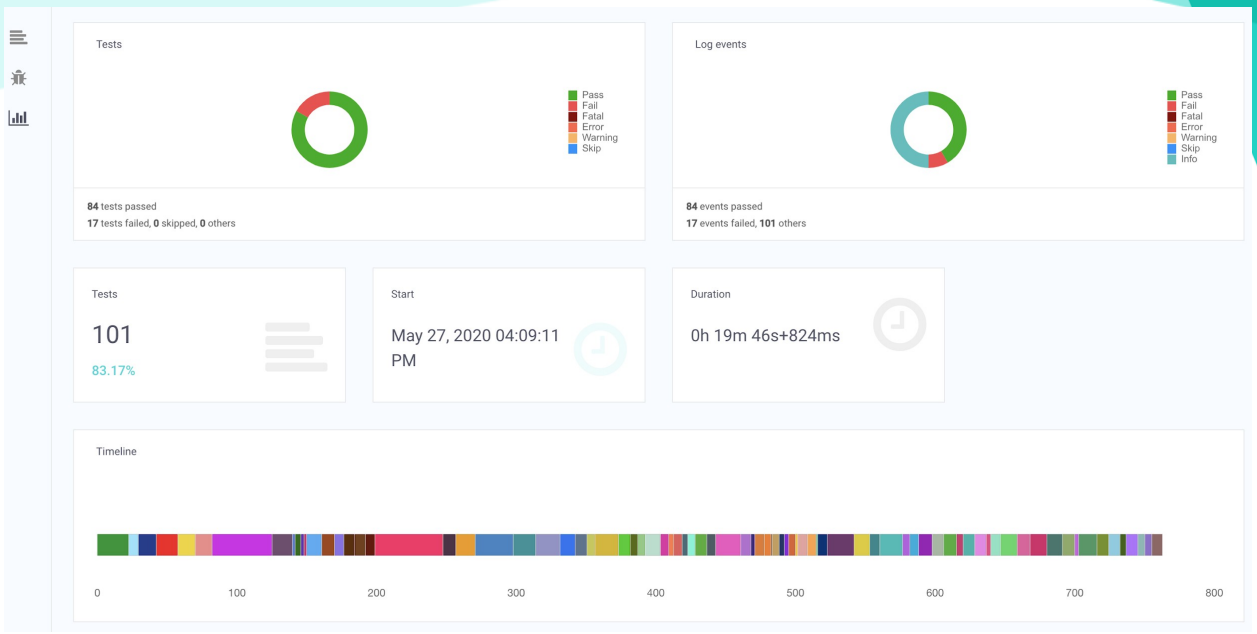
Not Required for Isolocity. Isolocity is an over-the-counter software.

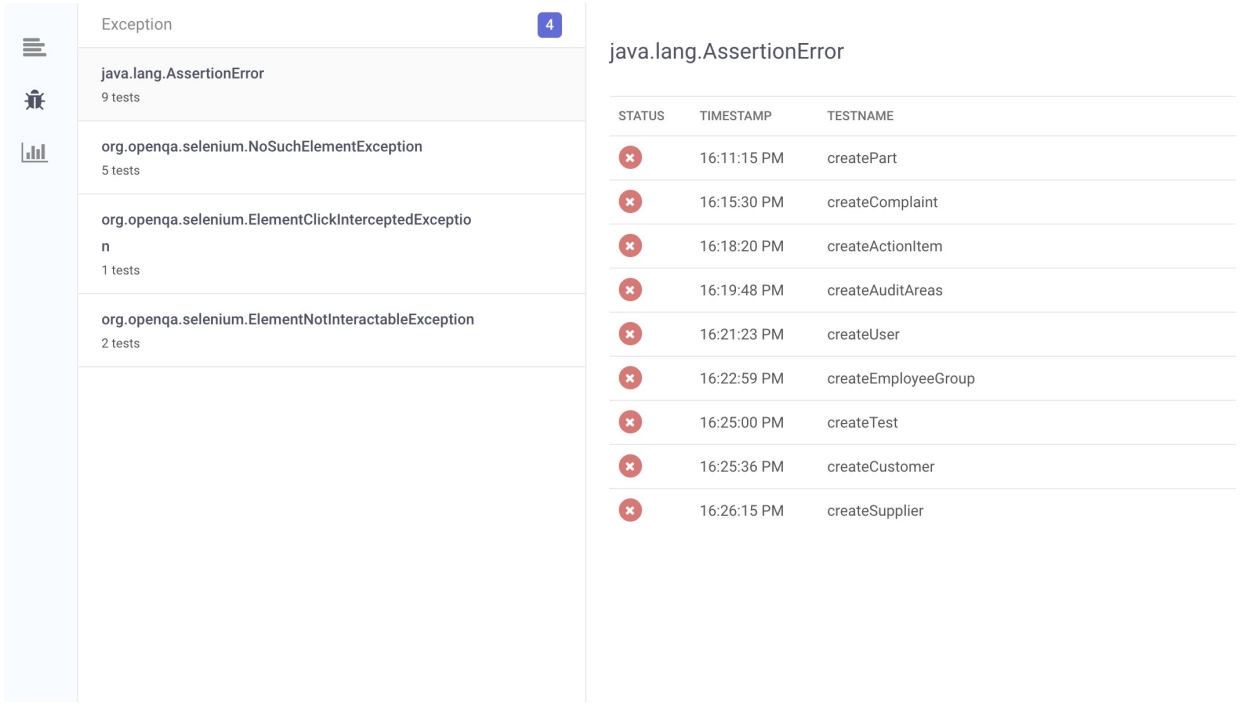
4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.

Along with our manual user driven testing utilizing the test cases in the link below, we also have an automated test suite that is running continuing.

https://docs.google.com/spreadsheets/d/15BUsOqqINAJRlboLUt5Z3cFxuq6rWTbApfbnbj7iX10/edit#gid=1494046008







4.8 If data is transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.

With all our integration partners, Isolocity and the partner conduct extensive testing prior to launching any integrated features. All applicable data transfers are identified here. https://docs.isolocity.com/

Operational Phase

5. Data

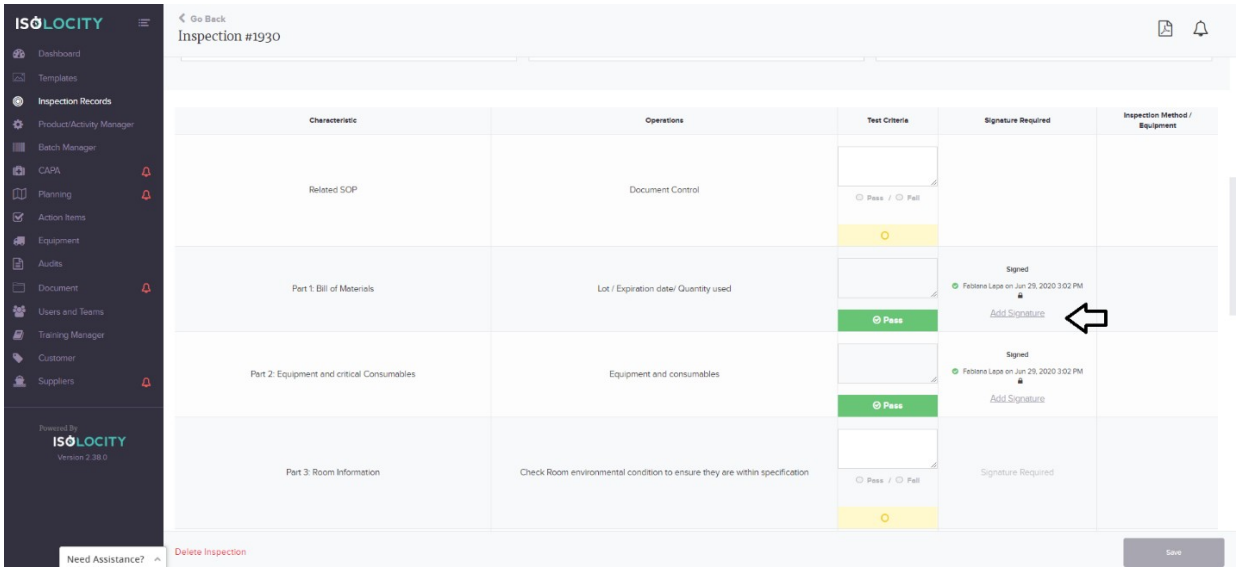
Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

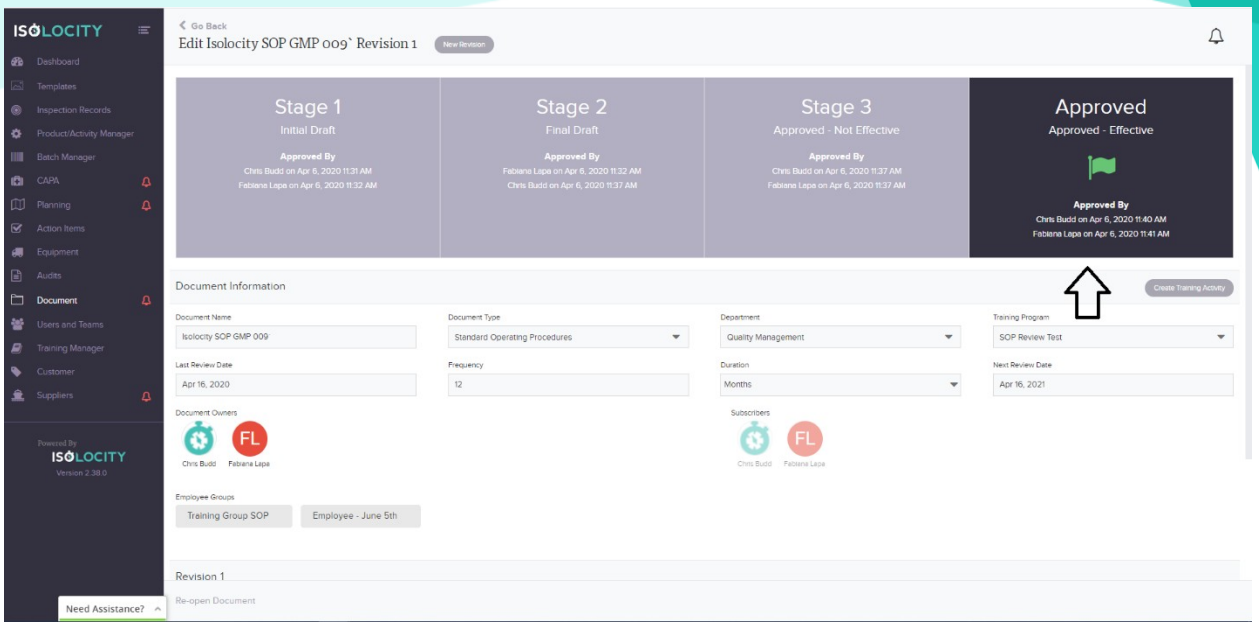
Isolocity integration- API calls are verified and validated through successful and rejected gateway codes.

6. Accuracy Checks

For critical data entered manually, there should be an additional check on the accuracy of the data. This check may be done by a second operator or by validated electronic means. The criticality and the potential consequences of erroneous or incorrectly entered data to a system should be covered by risk management.

2 signatures required

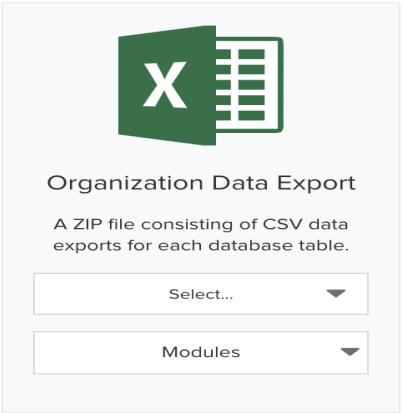




7. Data Storage

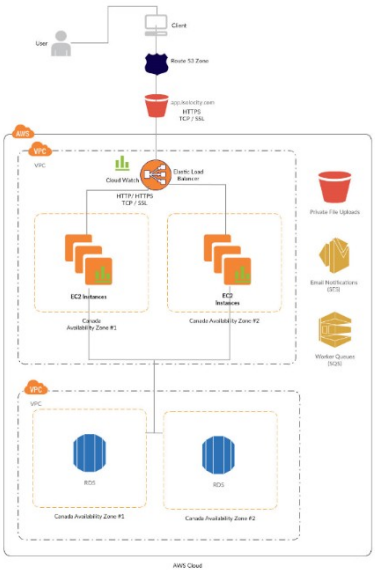
7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

AWS conducts regular backups. We verify all backup logs at regular frequencies. Furthermore, our clients databases can be exported upon request.



7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of backup data and the ability to restore the data should be checked during validation and monitored periodically.

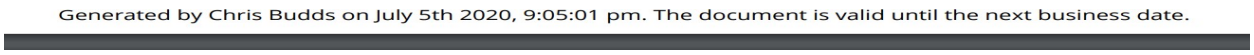
More info attached- AWS certificates.



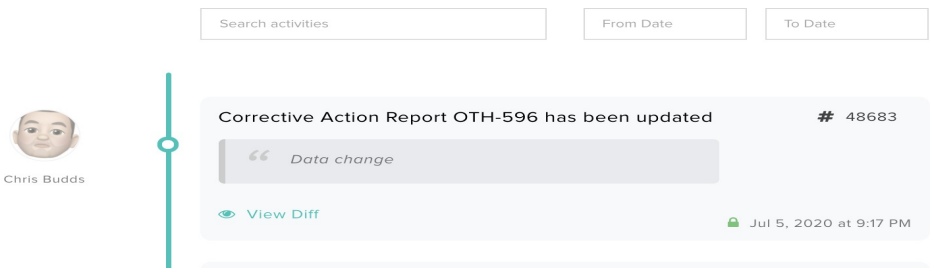
8. Printouts

8.1 It should be possible to obtain clear printed copies of electronically stored data.

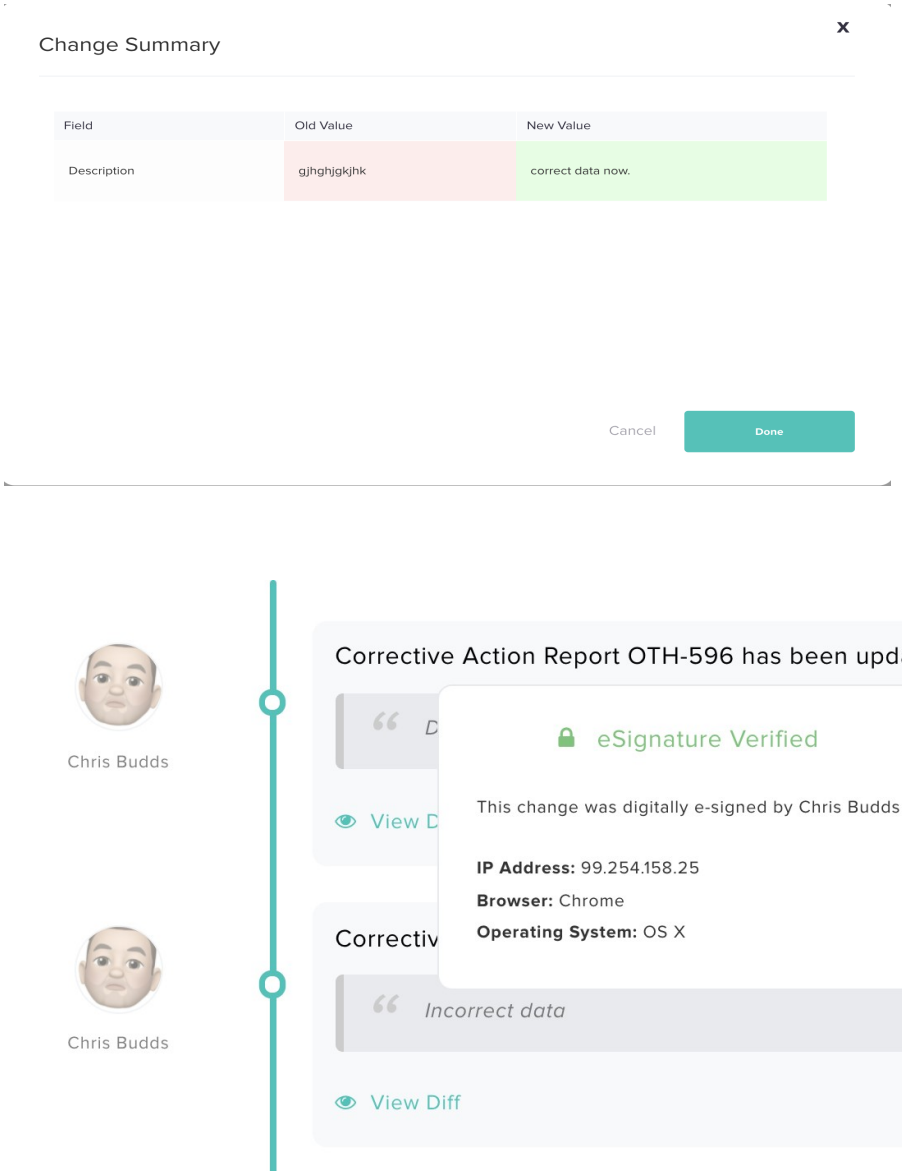
All modules, it is possible to download PDFs that provide a timestamp and expiration date on the PDF.



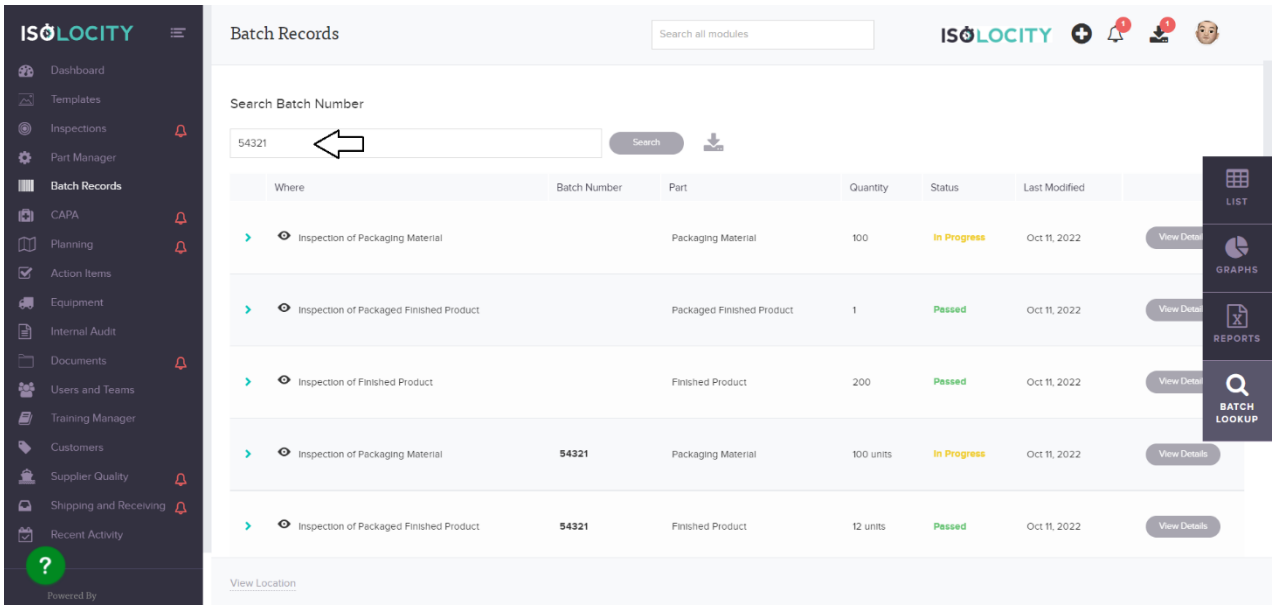
Every form has an activity tracker that provides an audit trail of all changes made.

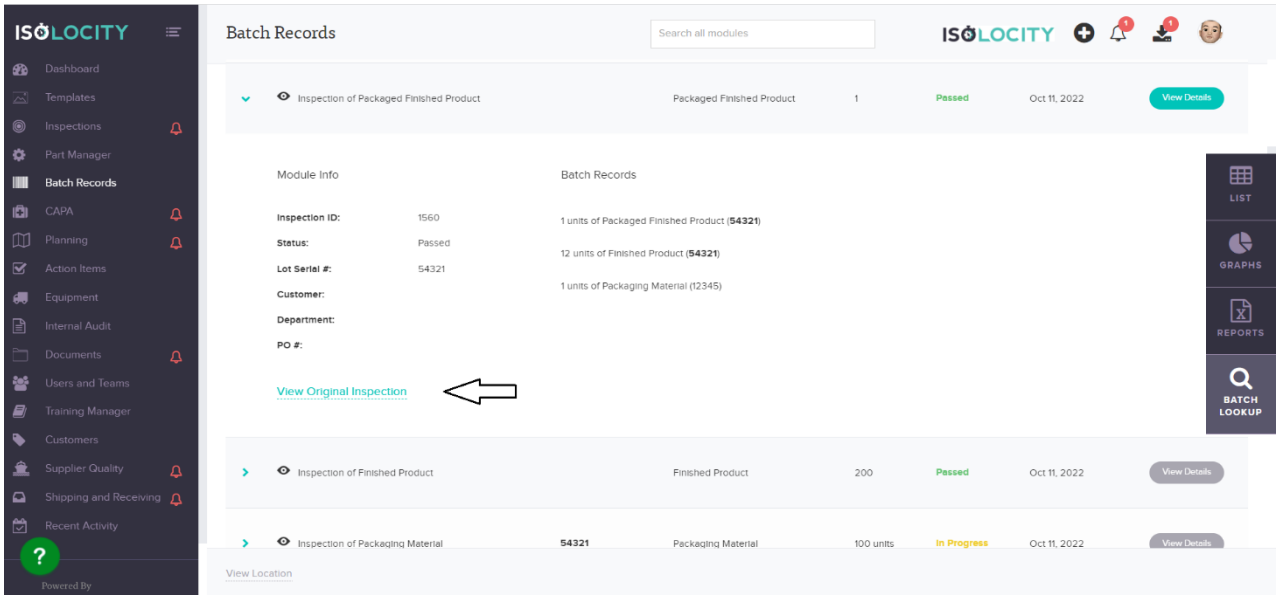


The changes to data are logged with a reason code along with e signature validation.



8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.





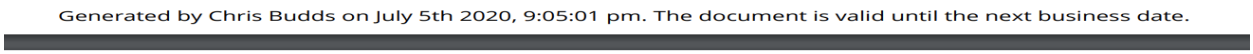
9. Audit Trails

Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").

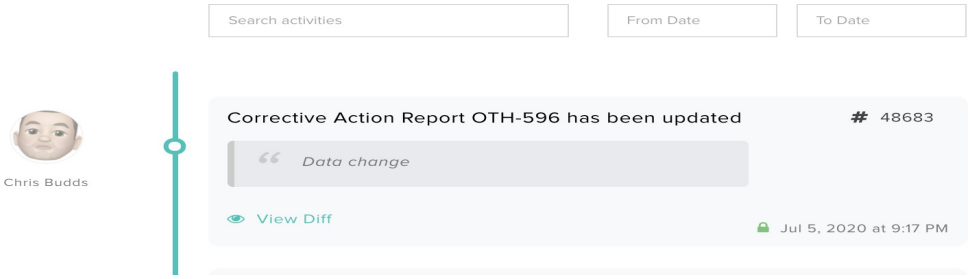
For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

See example from

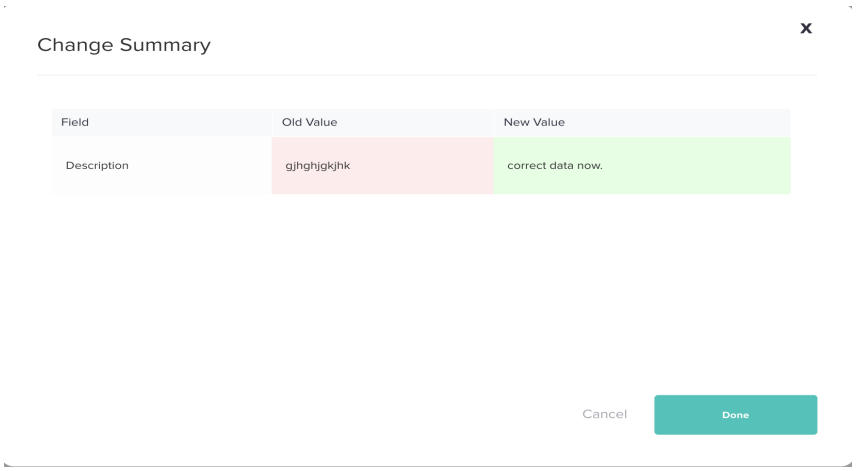
All modules, it is possible to download PDFs that provide a timestamp and expiration date on the PDF.

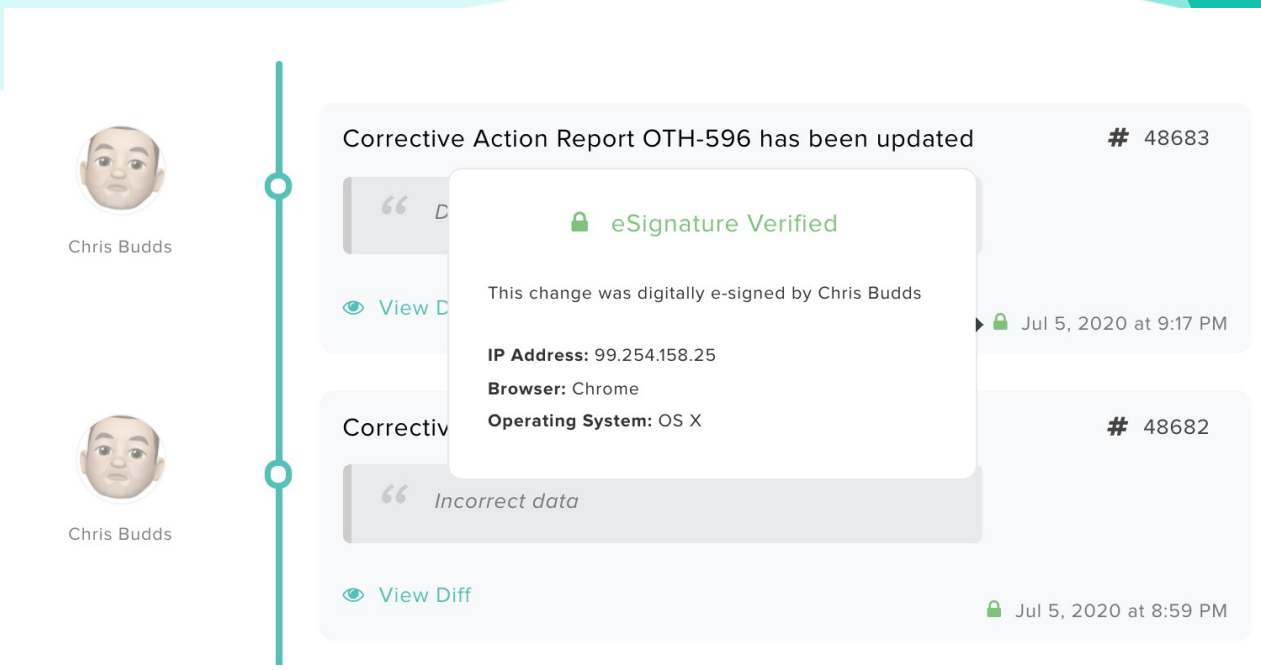


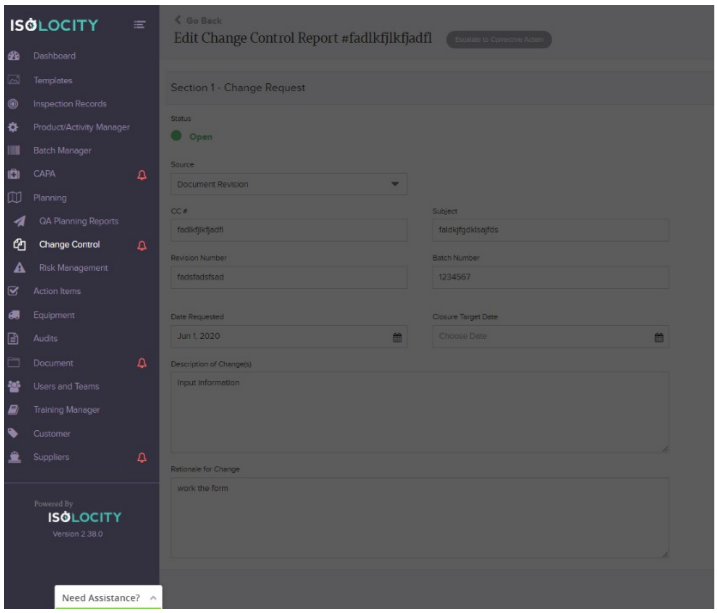
Every form has an activity tracker that provides an audit trail of all changes made.

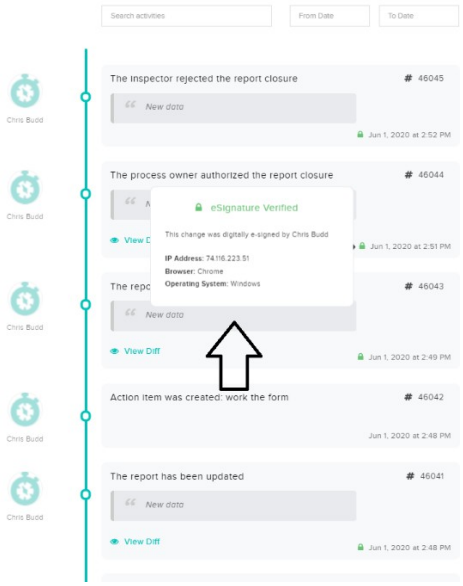


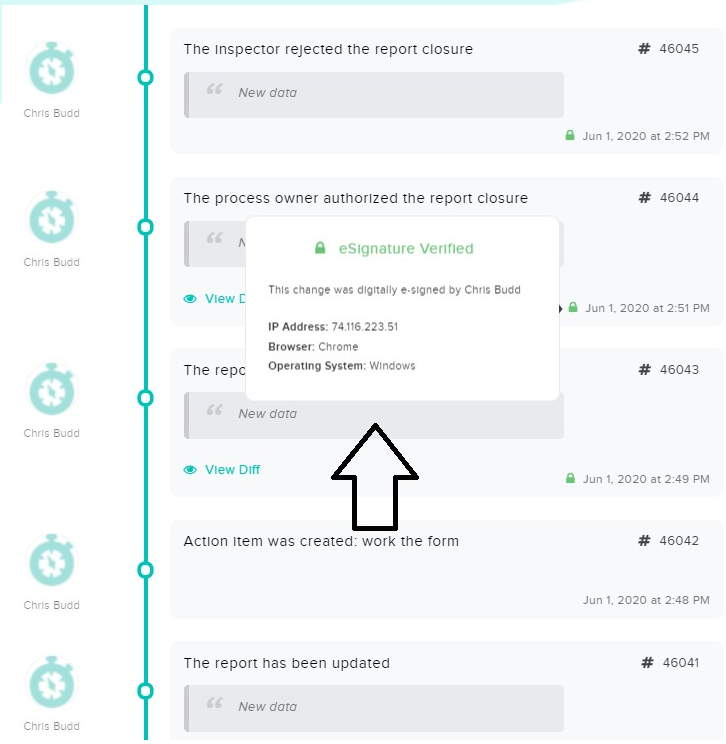
The changes to data are logged with a reason code along with e signature validation.




Chris Budds
Corrective Action Report OTH-596 has been updated
48683
eSignature Verified
This change was digitally e-signed by Chris Budds
IP Address: 99.254.158.25
Browser: Chrome
Operating System: OS X
View D
Jul 5, 2020 at 9:17 PM
Chris Budds
Correctiv
48682
Incorrect data
View Diff
Jul 5, 2020 at 8:59 PM

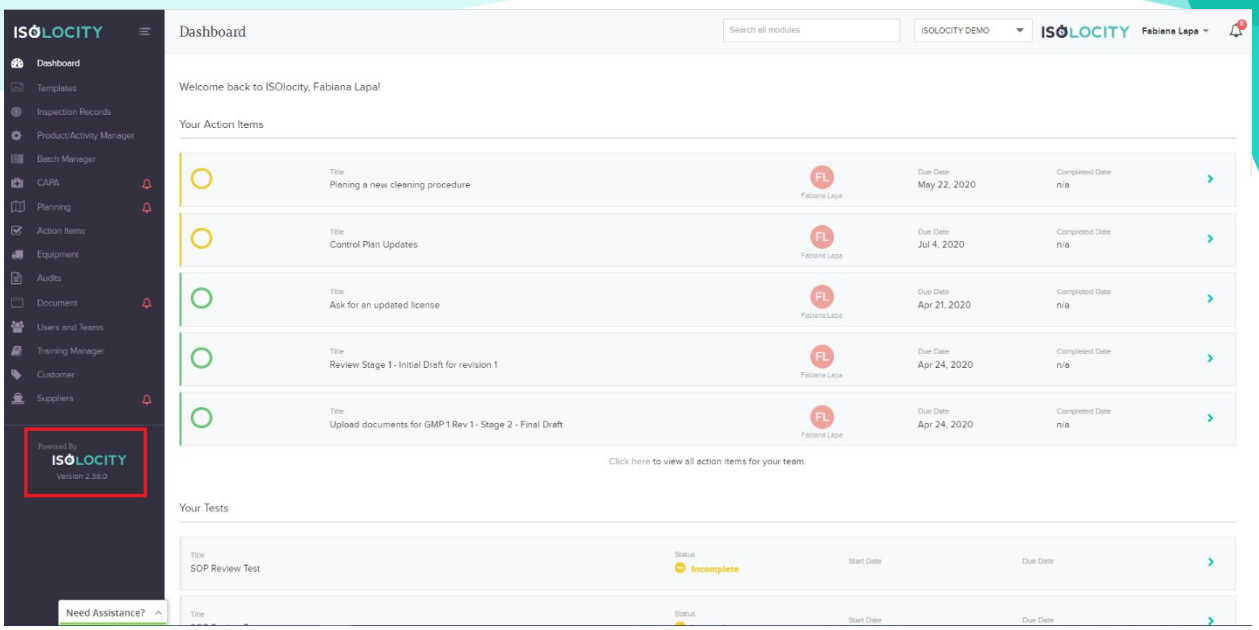

ISOLOCITY
Edit Change Control Report #fadlkfjlkfjadfl
Section 1 - Change Request
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Planning
QA Planning Reports
Change Control
Risk Management
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Need Assistance?


The inspector rejected the report closure
46045
The process owner authorized the report closure
46044
eSignature Verified
46043
View Diff
Action item was created: work the form
46042
The report has been updated
46041
New data



10. Change and Configuration Management Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

See Isolocity QP-11 Software validation.
All changes are version and revision controlled



11. Periodic evaluation Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

Once the software has been approved for operational use, routine maintenance may be performed to remove errors, to respond to new or modified equipment, or to adapt the software to changes in the operating environment. All planned changes must be approved by the Director of Operations before work is started. After any modifications, software must be verified and validated again.

Table A

Activity	3.1.1 Requirements Phase	Date/Initials
Task	Requirement Specification	
Method	Peer Review	
Check	Requirements Specification Approved	
Task	System Acceptance Test Specification	
Method	Peer Review	
Check	System Acceptance Test Specification Approved	

Table B

Activity	3.1.2 Design and Implementation Process	Date/Initials
Task	Design and Development Planning	
Method	Peer Review	
Task	Design Input	

Method	Peer Review	
Task	Design Output	
Method	Peer Review	
Task	Design Verification	
Method	Peer Review	
Task	Design Changes 1. Description: 2. Description:	
Method	Peer Review	

Activity	3.1.3 Construction Phase and 3.1.4 Testing Phase	Date/Initials
Task	Inspection Plan	
Method	Inspection	
Check	Inspection Approved	
Task	Test plan	
Method	Test Performance	
Check	Test Approved	

Table C

Activity	3.1.5 Installation and Validation Phase	Date/Initials
Task	Installation Summary	
Method	Peer Review	
Task	Installation Procedure	
Method	Verification and test of installation	
Task	System acceptance test preparation	
Method	System acceptance test	
Check	System acceptance test approved	

Table D

Activity	3.1.6 Documentation	Date/Initials
Task	Registered Anomalies	
Method	Peer Review	
Task	Precautionary Steps Taken	
Method	Verification of measures	

Table E

Activity	3.1.7 Operations and Maintenance	Date/Initials
Task	Performance and Maintenance	
Method	Peer Review	
Task	New Versions 1. Version: 2. Version:	
Method	Peer Review 1. Action: 2. Action:	

Task	Phase Out	
Method	Peer Review	

12. Security

12.1 Physical and/or logical controls should be in place to restrict access to computerised system to authorized persons. Suitable methods of preventing unauthorized entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

12.2 The extent of security controls depends on the criticality of the computerised system.

12.3 Creation, change, and cancellation of access authorizations should be recorded.

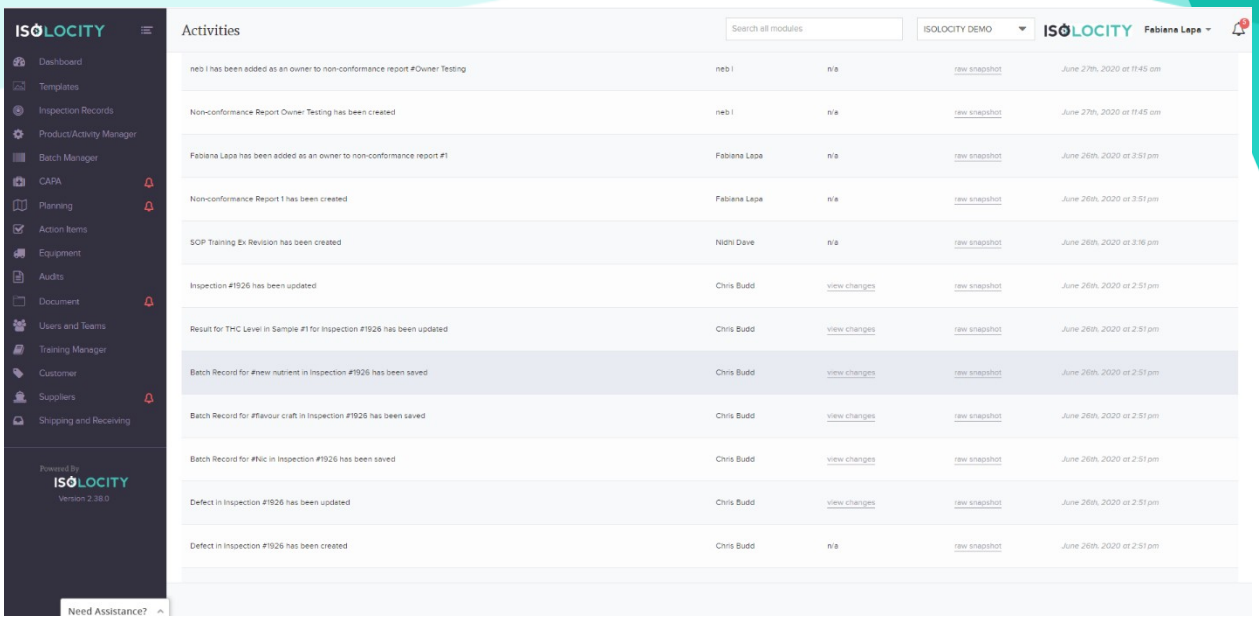
All user level changes, and access restrictions are recorded in our activity log.

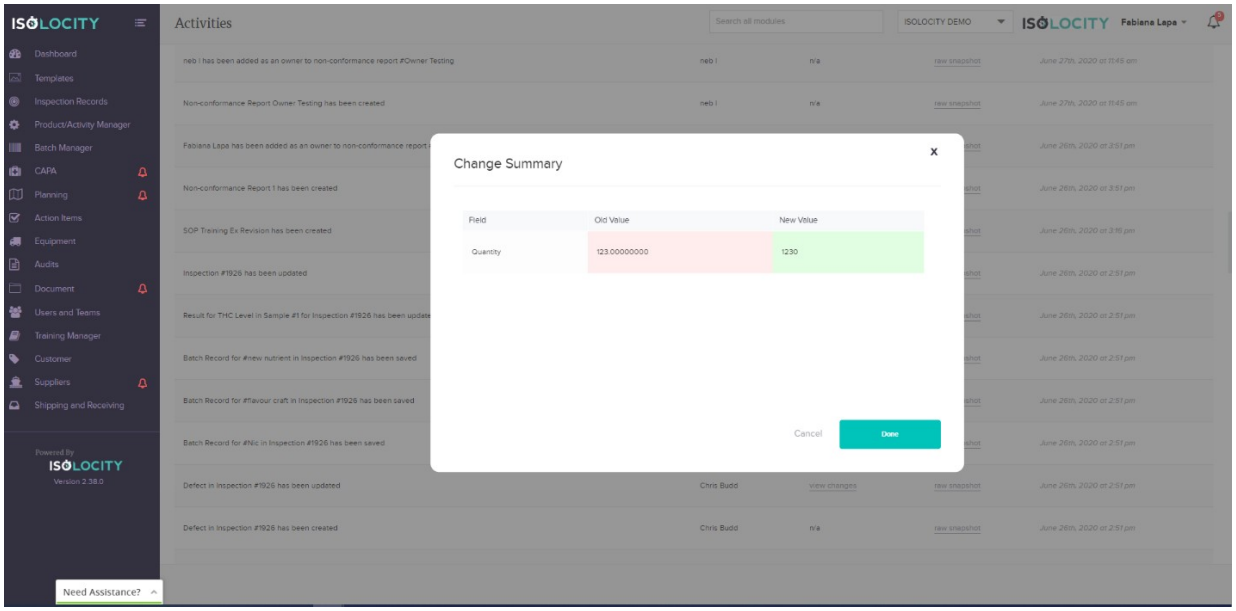
12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming, or deleting data including date and time.

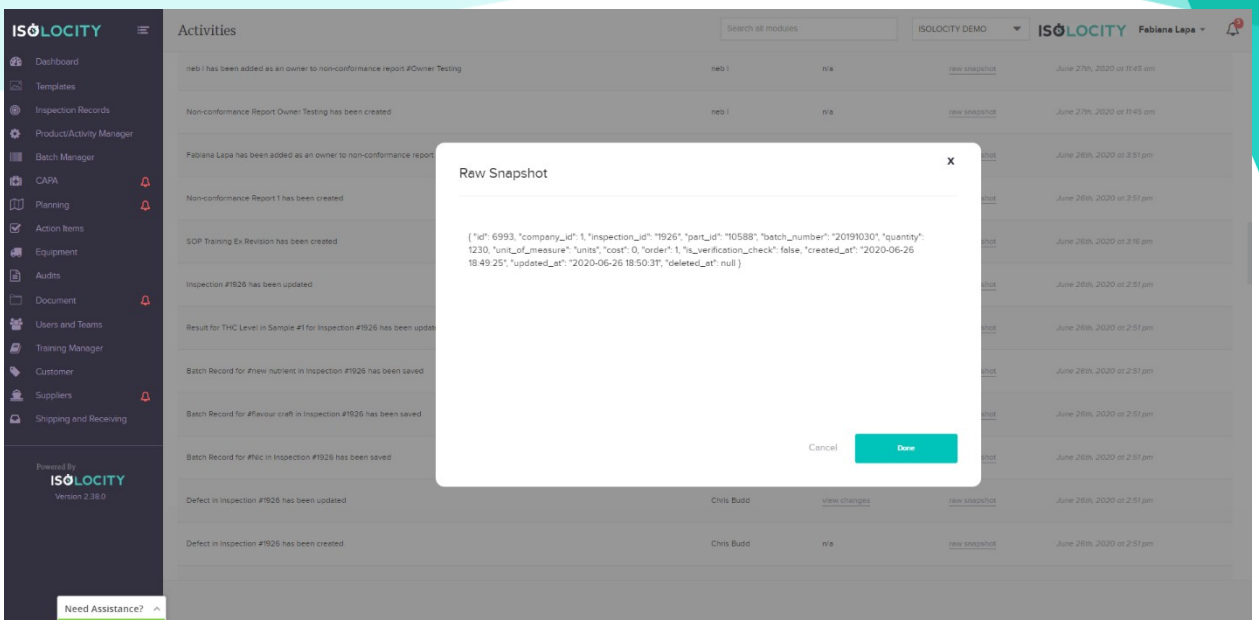
Isolocity User Tier & System Access | ISOLOCITY

	ADMIN	MANAGER	USER	PRODUCTION	EMPLOYEE
Module Access					
Inspections Criteria	✓	✓			
Inspection	✓	✓	✓	✓	
CAPA (CAPA/ NCR/ Deviations)	✓	✓	✓	✓	
Planning (Change Control/ risk/ planning reports)	✓	✓	✓		
Equipment	✓	✓	✓	✓	
Audits	✓	✓	✓		
Document Manager (Initiate Change Controls)	✓	✓	✓	✓	
HR Management	✓	✓			
Training Activities & Doc Training	✓	✓	✓	✓	✓
Data Permissions					
Create Users	✓				
Reopen Reports	✓				
Archive Info	✓				
Create Templates	✓	✓			
Create Training Programs	✓	✓			
Adjust Organizational Settings	✓				
Create Teams	✓				
Create Action Items	✓	✓	✓	✓	

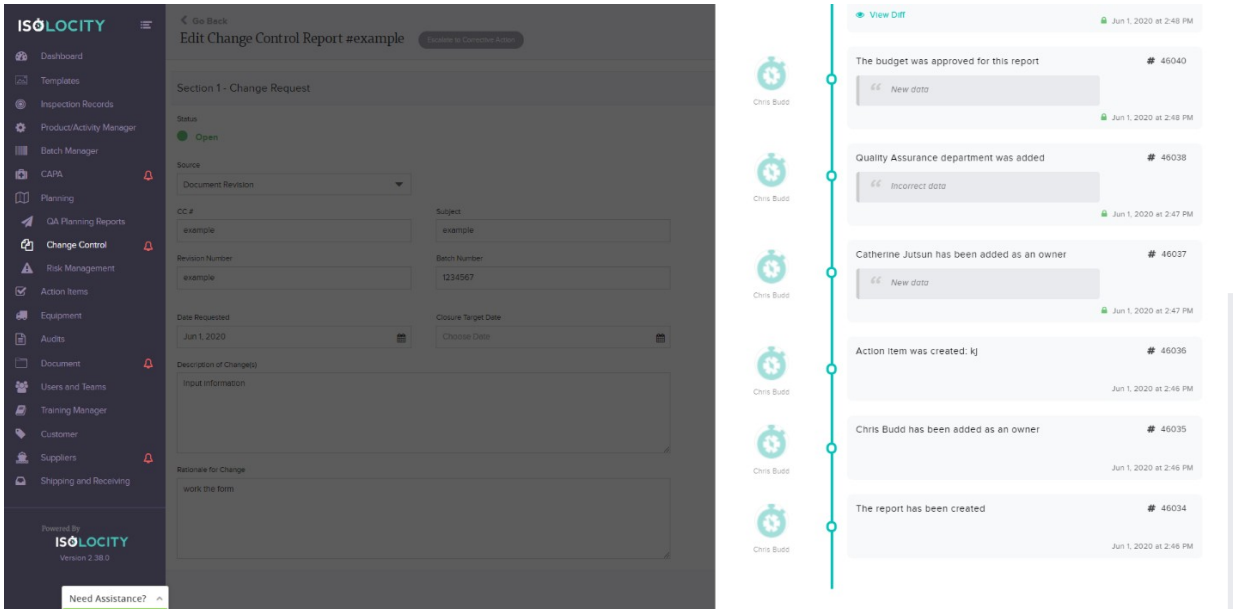
Recent activity:

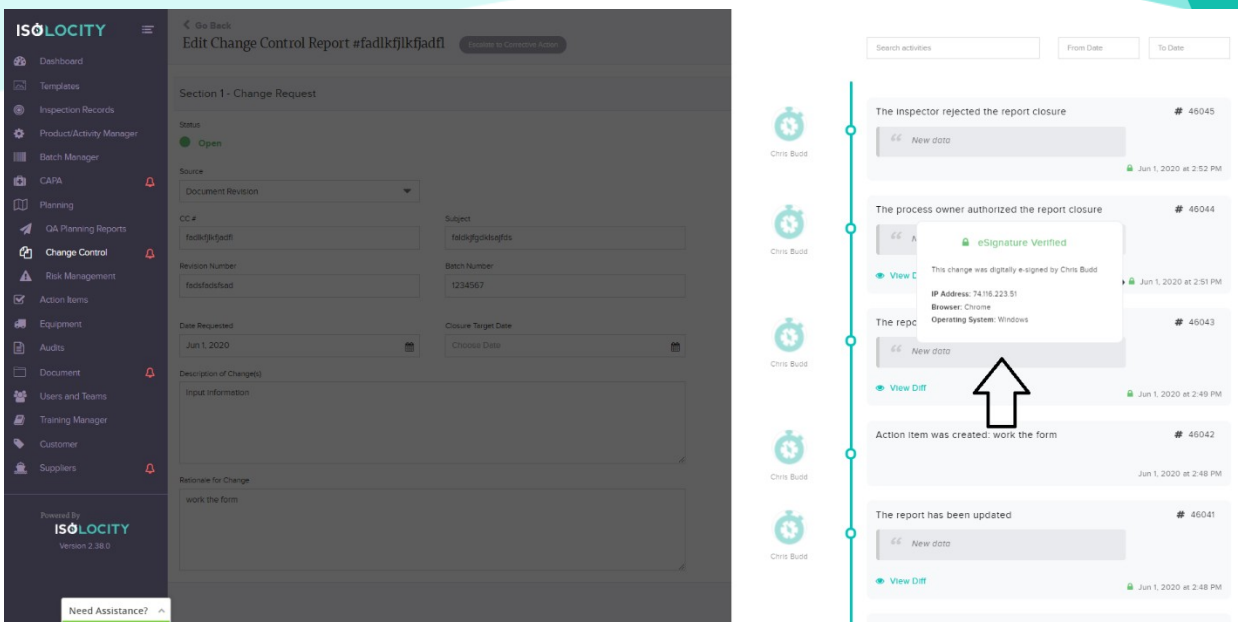

ISOLOCITY
Activities
Search all modules
ISOLOCITY DEMO
ISOLOCITY
Fabiana Lapa
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Planning
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Shipping and Receiving
Powered By
ISOLOCITY
Version 2.38.0
Need Assistance?
neb l has been added as an owner to non-conformance report #Owner Testing
Non-conformance Report Owner Testing has been created
Fabiana Lapa has been added as an owner to non-conformance report #1
Non-conformance Report 1 has been created
SOP Training Ex Revision has been created
Inspection #1926 has been updated
Result for THC Level in Sample #1 for Inspection #1926 has been updated
Batch Record for #new nutrient in Inspection #1926 has been saved
Batch Record for #flavour craft in Inspection #1926 has been saved
Batch Record for #Nic in Inspection #1926 has been saved
Defect in Inspection #1926 has been updated
Defect in Inspection #1926 has been created


ISOLOCITY
Activities
ISOLOCITY DEMO
ISOLOCITY
Fabiana Lapa
Change Summary
Field
Old Value
New Value
Quantity
123.00000000
1230
Cancel
Done
Need Assistance?



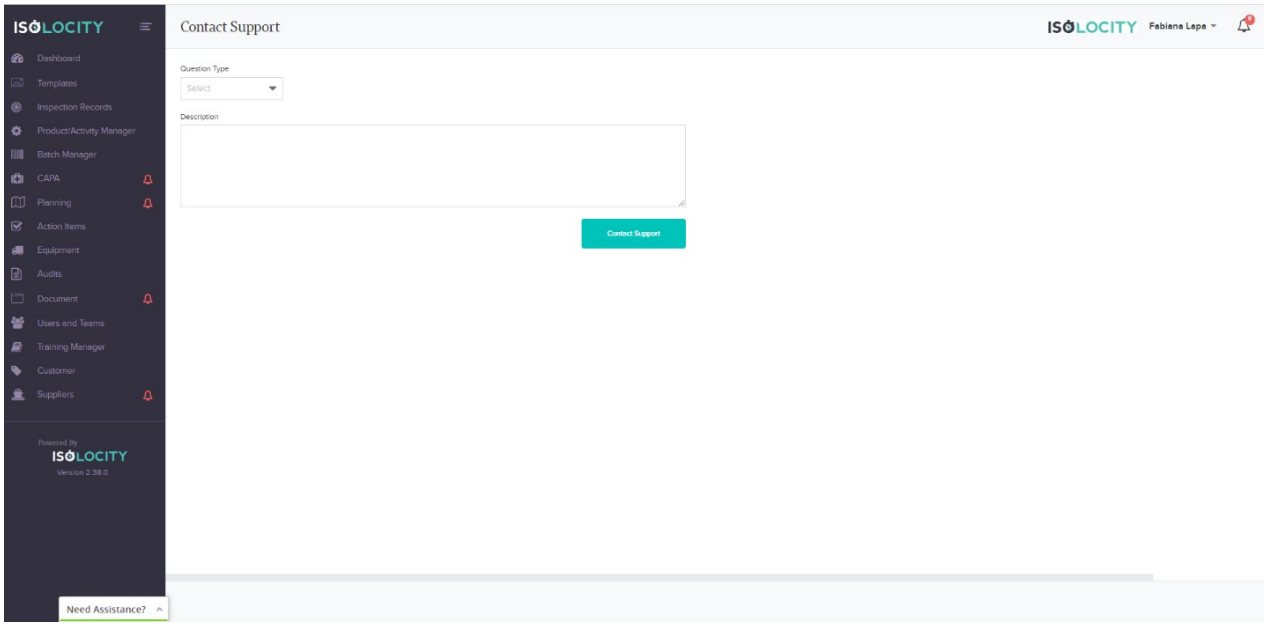
Change control:





13. Incident Management

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

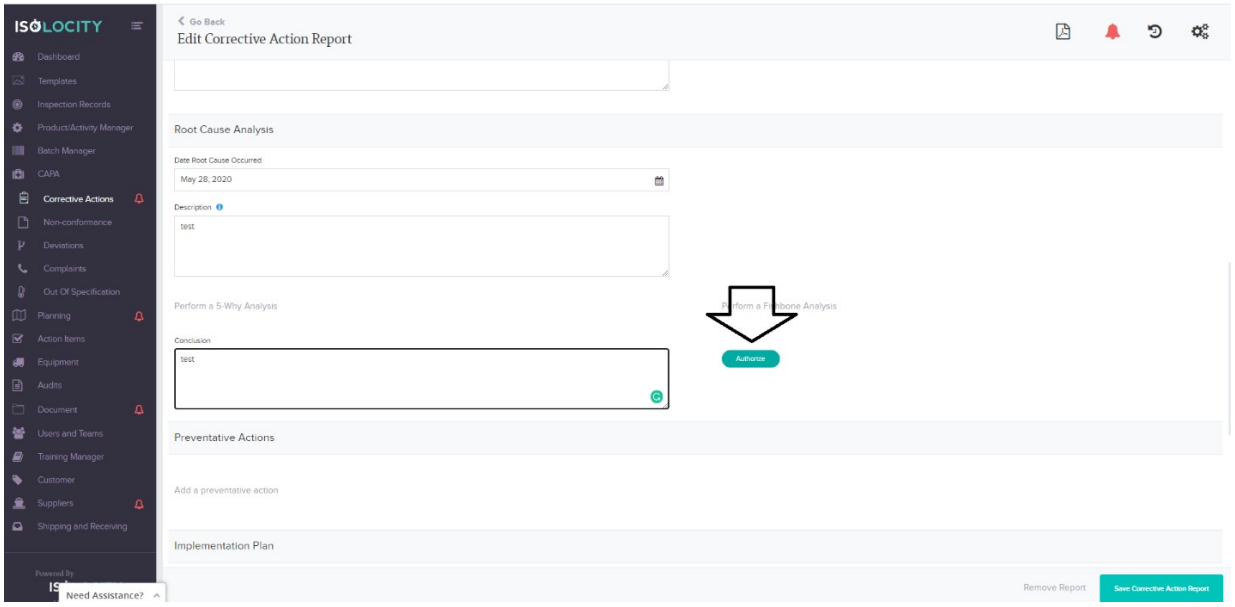


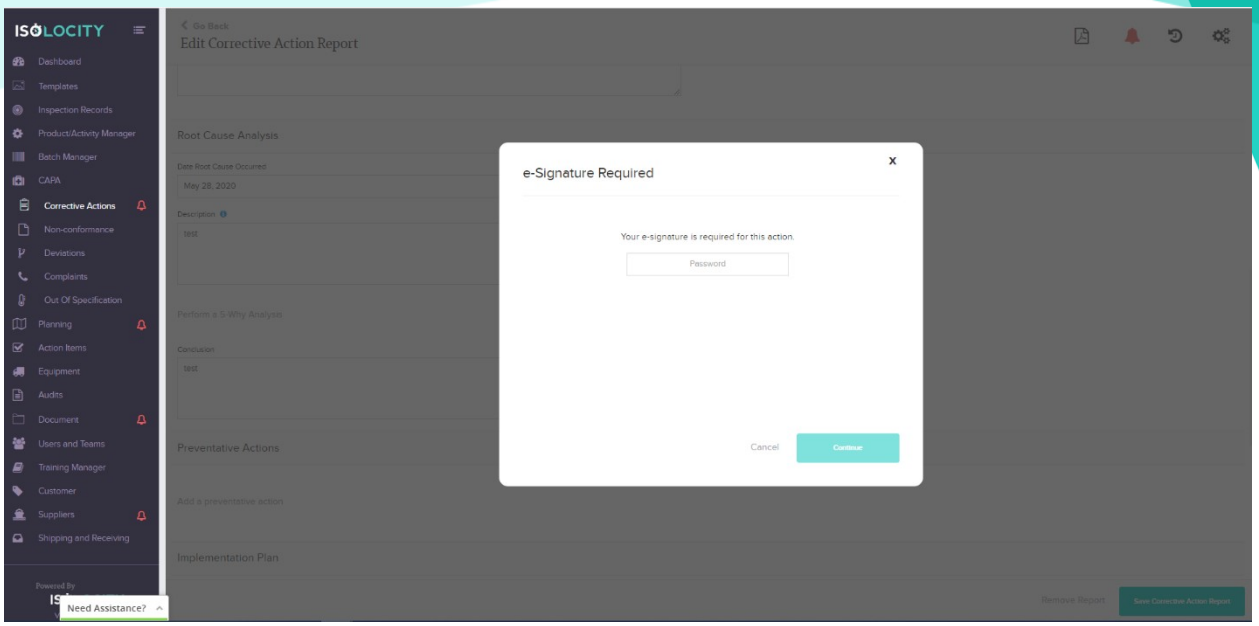
All Bugs follow an investigation and are documented in our client facing ticket system (Freshdesk) and are progressed to resolution using Asana. All bugs are provided with a rating; Critical, High, Medium and Low. All critical and High rated bugs are prioritized. As fixes are made to the

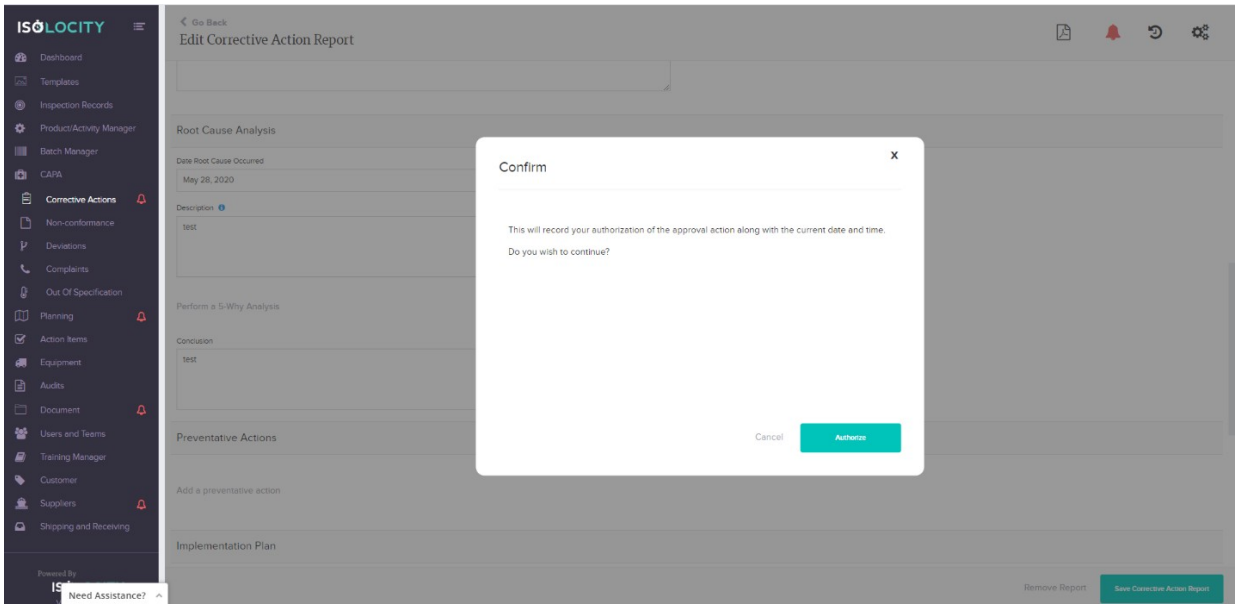
code and pushed to the User Accepted Testing site (UaT), all fixes are peer reviewed and QA by our head of QA. Once verified through automated regression testing, the code is then merged into the production servers.

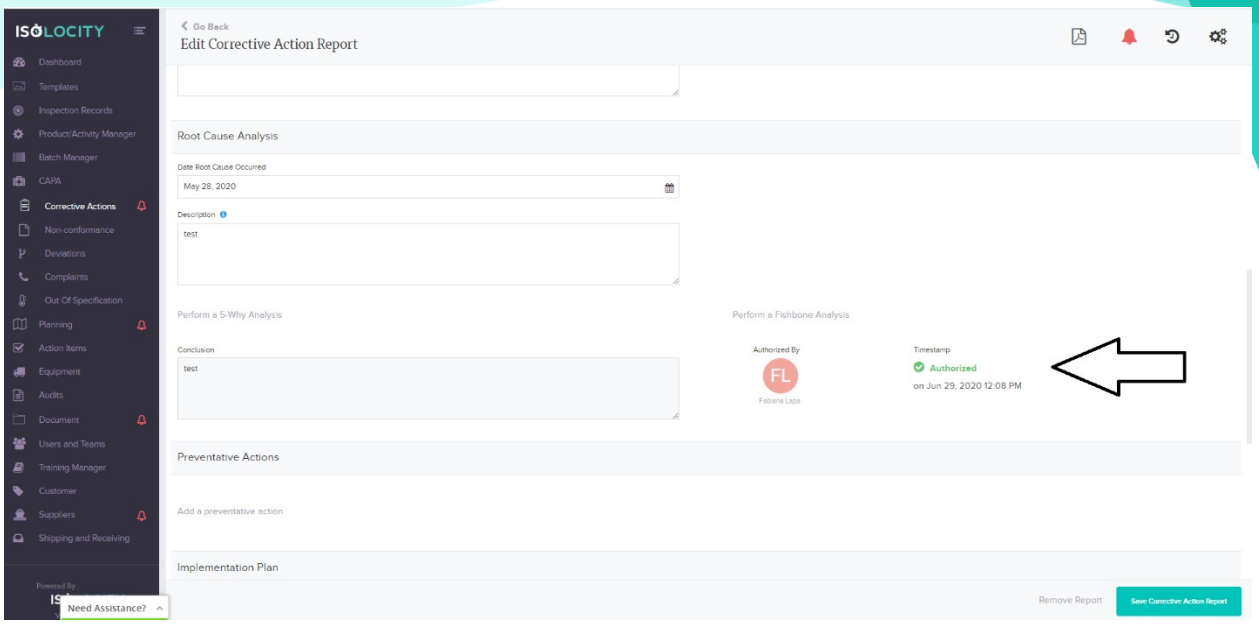
14. Electronic Signature

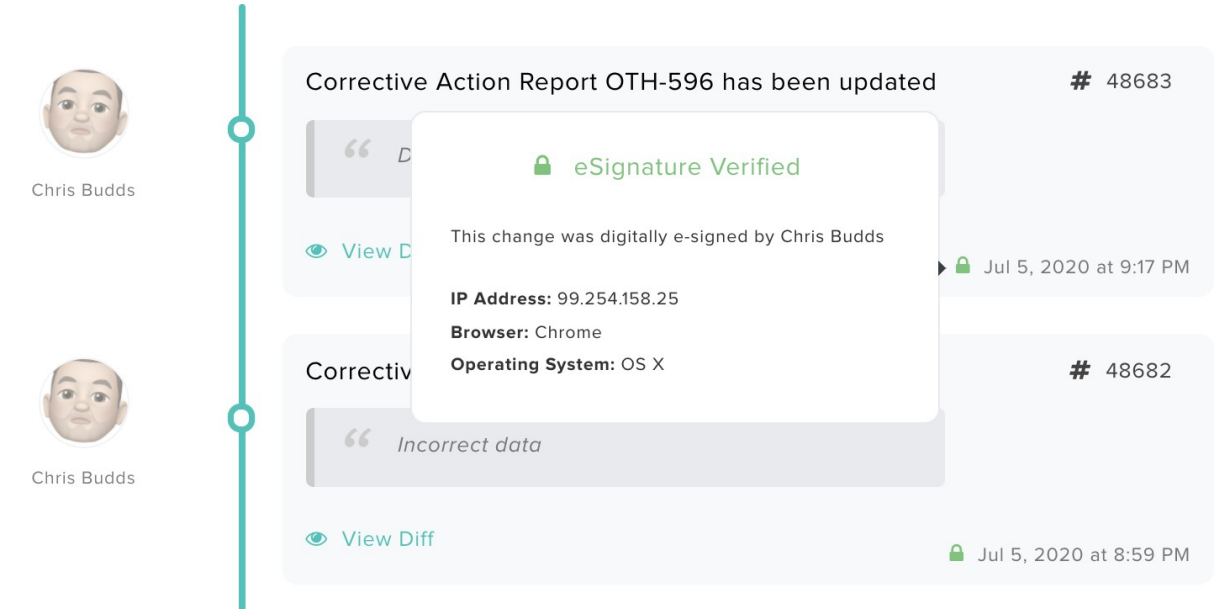
Electronic records may be signed electronically. Electronic signatures are expected to: a. have the same impact as hand-written signatures within the boundaries of the company, b. be permanently linked to their respective record, c. include the time and date that they were applied.




ISOLOCITY
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Corrective Actions
Non-conformance
Deviations
Complaints
Out Of Specification
Planning
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Shipping and Receiving
Need Assistance?
Go Back
Edit Corrective Action Report
Root Cause Analysis
Date Root Cause Occurred
May 28, 2020
Description
test
Perform a 5-Why Analysis
Conclusion
test
Preventative Actions
Add a preventative action
Implementation Plan
Remove Report
e-Signature Required
Your e-signature is required for this action.
Password
Cancel
Continue

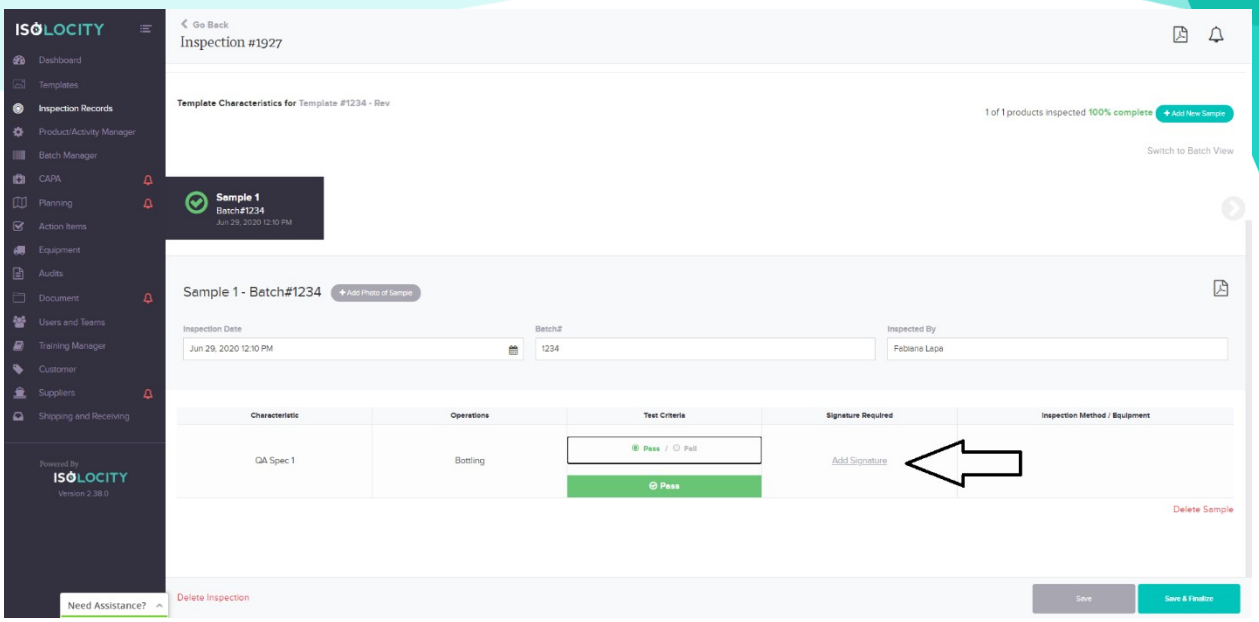

ISOLOCITY
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Corrective Actions
Non-conformance
Deviations
Complaints
Out Of Specification
Planning
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Shipping and Receiving
Need Assistance?
Go Back
Edit Corrective Action Report
Root Cause Analysis
Date Root Cause Occurred
May 28, 2020
Description
test
Perform a 5-Why Analysis
Conclusion
test
Preventative Actions
Add a preventative action
Implementation Plan
Remove Report
Save Corrective Action Report
Confirm
This will record your authorization of the approval action along with the current date and time.
Do you wish to continue?
Cancel
Authorize

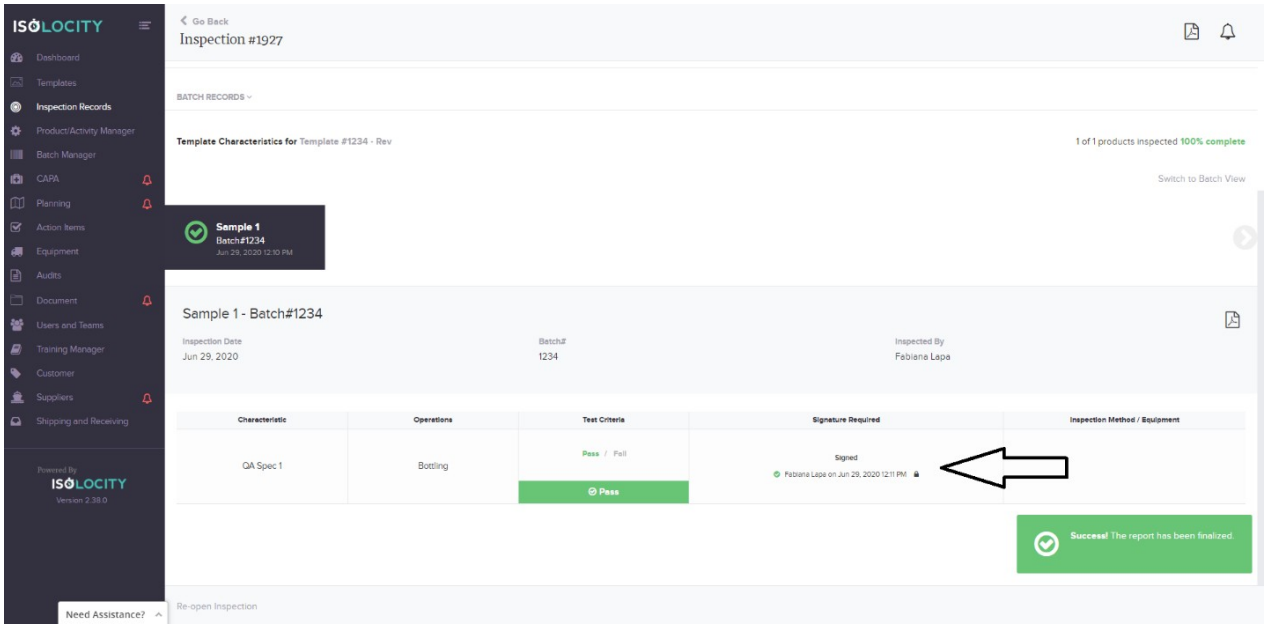




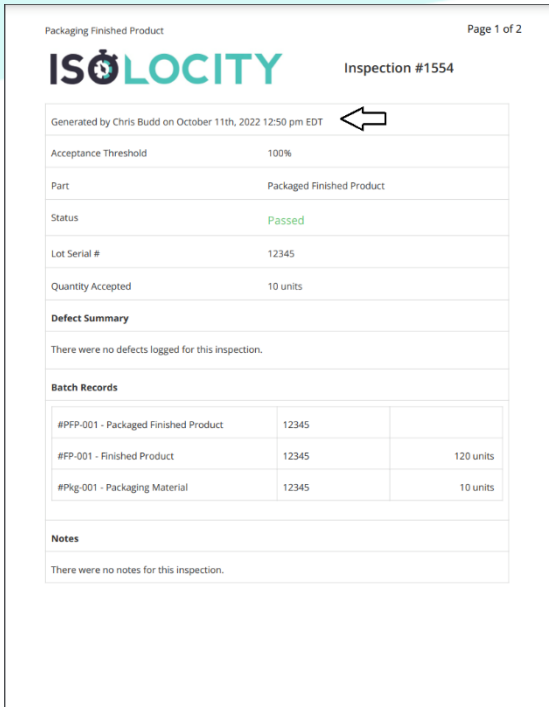
15. Batch release

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.


ISOLOCITY
Go Back
Inspection #1927
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Planning
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Shipping and Receiving
Powered By ISOLOCITY Version 2.38.0
Need Assistance?
Template Characteristics for Template #1234 - Rev
1 of 1 products inspected 100% complete
+ Add New Sample
Switch to Batch View
Sample 1
Batch#1234
Jun 29, 2020 12:10 PM
Sample 1 - Batch#1234
+ Add Photo of Sample
Inspection Date
Jun 29, 2020 12:10 PM
Batch#
1234
Inspected By
Fabiana Lapa
Characteristic
Operations
Test Criteria
Signature Required
Inspection Method / Equipment
QA Spec 1
Bottling
Pass / Fail
Pass
Add Signature
Delete Sample
Delete Inspection
Save
Save & Finalize


ISOLOCITY
Go Back
Inspection #1927
BATCH RECORDS
Dashboard
Templates
Inspection Records
Product/Activity Manager
Batch Manager
CAPA
Planning
Action Items
Equipment
Audits
Document
Users and Teams
Training Manager
Customer
Suppliers
Shipping and Receiving
Powered By ISOLOCITY Version 2.38.0
Need Assistance?
Template Characteristics for Template #1234 - Rev
1 of 1 products inspected 100% complete
Switch to Batch View
Sample 1
Batch#1234
Jun 29, 2020 12:10 PM
Sample 1 - Batch#1234
Inspection Date
Jun 29, 2020
Batch#
1234
Inspected By
Fabiana Lapa
Characteristic
Operations
Test Criteria
Signature Required
Inspection Method / Equipment
QA Spec 1
Bottling
Pass / Fail
Pass
Signed
Fabiana Lapa on Jun 29, 2020 12:11 PM
Success! The report has been finalized.
Re-open Inspection

PDF Report:



Packaging Finished Product

Page 1 of 2

ISOLOCITY

Inspection #1554

Generated by Chris Budd on October 11th, 2022 12:50 pm EDT

Acceptance Threshold	100%
Part	Packaged Finished Product
Status	Passed
Lot Serial #	12345
Quantity Accepted	10 units

Defect Summary

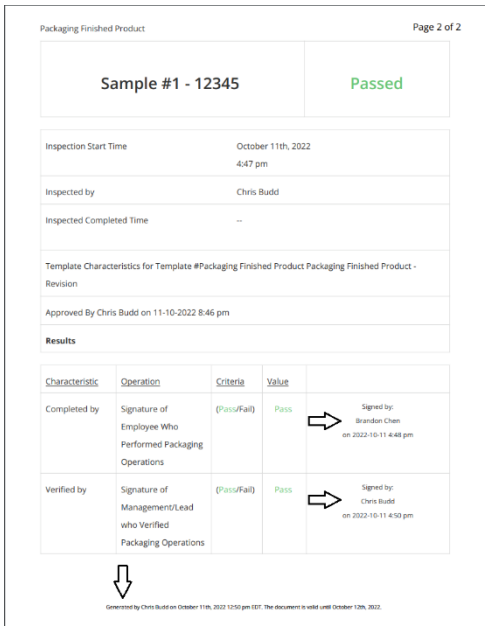
There were no defects logged for this inspection.

Batch Records

#PFP-001 - Packaged Finished Product	12345	
#FP-001 - Finished Product	12345	120 units
#Pkg-001 - Packaging Material	12345	10 units

Notes

There were no notes for this inspection.



Packaging Finished Product

Page 2 of 2

Sample #1 - 12345

Passed

Inspection Start Time	October 11th, 2022 4:47 pm
Inspected by	Chris Budd
Inspected Completed Time	--

Template Characteristics for Template #Packaging Finished Product Packaging Finished Product - Revision

Approved By Chris Budd on 11-10-2022 8:46 pm

Results

Characteristic	Operation	Criteria	Value	
Completed by	Signature of Employee Who Performed Packaging Operations	(Pass/Fail)	Pass	Signed by: Brandon Chen on 2022-10-11 4:48 pm
Verified by	Signature of Management/Lead who Verified Packaging Operations	(Pass/Fail)	Pass	Signed by: Chris Budd on 2022-10-11 4:50 pm

Generated by Chris Budd on October 11th, 2022 12:50 pm EDT. The document is valid until October 12th, 2022.

16. Business Continuity

For the availability of computerised systems supporting critical processes, provisions should be made to ensure continuity of support for those processes in the event of a system breakdown (e.g. a manual or alternative system). The time required to bring the alternative arrangements into use should be based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.

This is a client driven process. Should have a paper-based system for back up.

17. Archiving

Data may be archived. This data should be checked for accessibility, readability, and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

Isolocity provides archive folders for clients to store completed or obsolete data. Isolocity does not archive any data automatically, unless requested by the client.

Glossary

Application: Software installed on a defined platform/hardware providing specific functionality

Bespoke/Customized computerised system: A computerised system individually designed to suit a specific business process

Commercial of the shelf software: Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users.

IT Infrastructure: The hardware and software such as networking software and operation systems, which makes it possible for the application to function.

Life cycle: All phases in the life of the system from initial requirements until retirement including design, specification, programming, testing, installation, operation, and maintenance.

Process owner: The person responsible for the business process.

System owner: The person responsible for the availability, and maintenance of a computerised system and for the security of the data residing on that system.

Third Party: Parties not directly managed by the holder of the manufacturing and/or import authorization.