Honeywell

Compliance in the BioPharma Industry

White Paper v1.0

July 2005

I. Introduction

In the BioPharma industry, it's becoming increasingly important that systems support the processes of the company. There are many ways in this heavily regulated industry in which a company can inadvertently step out of compliance. Honeywell builds its systems to serve these industries. By designing systems that help support compliance with these regulations, Honeywell makes it easier for companies to ensure that their processes are doing exactly what they are supposed to do.

Today, Honeywell offers Pro-Watch as the integrated security system software for regulated industries. The technology incorporated into Pro-Watch is derived from thirty years of experience in the process and FDA regulated industries. This depth of experience gives Pro-Watch a unique set of features ideally suited for the FDA regulated industries.

While the use of electronic signatures and electronic records, as well as their submission to FDA, is voluntary, electronic signatures and electronic records have several advantages over paper systems. This includes having automated databases capable of advanced automatic searches of information; allowing information to be viewed from multiple perspectives; permitting determination of trends, patterns and behaviors; and, avoiding document misfiling.

A product or device, by definition, cannot be compliant because the validation criteria depends on the customer's processes and how they will operate and maintain the systems they have. However, Honeywell's Pro-Watch software provides features that facilitate validation and 21CFR Part 11 compliance. This document provides an overview of Pro-Watch capabilities as they relate to system validation.

II. Overview of Regulations

Compliance is playing an increasingly powerful role in corporate planning for BioPharma companies and indeed all industries. Regulations aimed at the methods organizations use to secure, document and protect their data and systems have changed the way we think about business. Legislation such as the Gramm-Leach Bliley Act (GLB), Health Care Information Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act (SOX), and Title 21 Code of Federal Regulations (21CFR Part 11 FDA) were all motivated by different circumstances and each have its own unique requirements. However, from a security management perspective, these requirements can be largely grouped into the following three categories:

- Ensure that data can only by accessed by authorized individuals
- Ensure that data is accurate and is readily available to those who are authorized to access it

- Ensure that processes are in place to comply with the first two

The Food and Drug Administration (FDA) is the primary regulatory agency providing guidelines to the BioPharma market. In 1997, the FDA developed *Title 21CFR Part 11*, a uniform approach to regulating record keeping, reporting and electronic signature practices for all business functions under its control. This regulation has far-reaching implications for all businesses within the BioPharma industry, as well as other regulated industries like Food and Beverage. Some of the mandates include:

- Accounting for storage and use of identity data
- Certifying the identity of those who access certain information
- Understanding what is being done with the information
- Proving who/what/why/where/how in an audit

Global growth is a necessity in order to be competitive within the BioPharma industry and has significant implications for security. Establishing standard procedures which can be followed and enforced across multiple locations reduces time and resources required for investigation of incidents. The ability to scale the security system in the face of rapid expansion is a critical component as well.

III. Overview of Validation

a. Validation

Today, certain parts of a pharmaceutical enterprise contain "validated" areas. These include everything from the physical locations for manufacturing, laboratories and storage to the locations on the data systems that support these functions. The aim of validation is to ensure that the user's needs and intended objectives can be fulfilled on a consistent, repeatable and predictable basis.

Validation is defined as establishing documented evidence that provides a high degree of assurance that a specific process will consistently operate in accordance with pre-defined specifications. This means that there is no such thing as validated devices or equipment, but rather continuous processes that support validated systems. The purpose therefore is to prove with a high degree of assurance that it will work correctly and consistently. For 21CFR Part 11 compliance, validation should also prove the accuracy and reliability of the data collection and management system. Figure 12 illustrates the general validation activities that need to be completed. It progresses logically from specification through the review of results.

As such, a Validation Master Plan (VMP) or set of validation protocols is required to describe how the overall system will be setup, run and maintained so that the system performs as expected in a consistent manner. This VMP is highly dependent on the individual customer requirements and, as such, must be defined by the customer, not by system capabilities. Areas of focus may include maintenance, training, change control, data integrity and storage, security and disaster recovery. Generally speaking, the customer is responsible for creating and maintaining the VMP or validation protocols. However, Honeywell may provide assistance to customers in helping them develop these documents (for more details on VMP and how Honeywell can help prepare one for you, please see our Professional Services in a Validated Environment document).

Developing documented evidence has traditionally consisted of the following:
Planning – Preparing a written validation plan.
Specifications – Specifying and agreeing on what is required.
Test Planning – Preparing documents that describe how the equipment/system it to be tested.

Testing – Performing the planned tests and collecting the results.
Review – Reviewing the results to show that the system performs as specified.

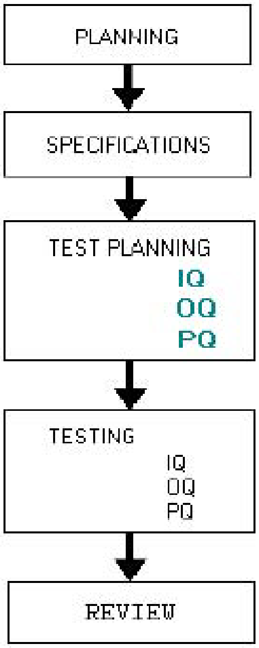

Figure 1: General Validation Activities

b. Security's Part Within Validation

The structure and design of a security system provides some fundamental strengths for solidifying validation across the enterprise. Because security is designed to control access to areas and information in a structured manner, it is a good foundation on which to build specific tools for compliance.

Restriction of Physical Access

Validated systems must be able to restrict both physical and logical access to the appropriate areas. There are many different regulations specifying physical access control. The Pro-Watch System was built up from an access control system and is designed to differentiate levels of access for a variety of physical locations. The system can restrict access not just based on user profiles, but also on time, previous location, etc.

Restriction of Logical Access

Validated systems must be able to restrict system access to only those users that are approved to enter. Pro-Watch has password-controlled access for all users. Additionally, user profiles can be set to automatically define areas of access and permitted activities within the system.

Maintenance and Change Control

For validated systems, it is incredibly important that the system be designed both with audit log capabilities and configured with sufficient storage to make necessary data available. The locking of these audit logs so that they cannot be modified by anyone, even an administrator, is a key function of the Pro-Watch system. Every change to the data and to the system itself is recorded in these logs. All of these changes are also recorded with time and for manual changes with the operator ID.

Both the new and the old data must be maintained so that changes do not obscure the old records. Pro-Watch is designed to track the history of these changes. Once these logs have been archived, the records are permanent. Reports can be generated on all of this information, but in a read-only format.

Training

Although training is generally covered under operational procedures, Honeywell's Pro-Watch provides assistance in making sure only trained personnel are using the system. Operators on the system have a profile that contains information on their security level, control level, area assignments and starting display. Areas can be used as a way of segregating operators to only seeing and controlling parts of the process on which they have been trained. When that training occurs, they can then have that area added to their profile.

IV. Introduction to 21CFR Part 11

a. *Purpose*

The objective of 21CFR Part 11 is to create criteria for electronic record keeping while preserving the FDA's ability to protect and promote the public health. Part 11 defines criteria under which the FDA considers electronic records and electronic signatures to be trustworthy, reliable and generally equivalent to paper records and handwritten signatures.

Passed into law in 1997, 21CFR Part 11 was designed to benefit both the FDA and the manufacturers that it regulates. Part 11 was designed to increase speed of information exchange, reduce document storage space and reduce errors in record keeping. It applies to those records and signatures required by FDA predicate rules, including signatures that are not required but appear in required documents.

Current FDA regulations for the use of electronic systems require that persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of the traditional handwritten signatures.

Considering Part 11 requirements when developing a project validation plan or quality plan will facilitate compliance.

b. *Definitions*

Electronic Record: Any combination of text, graphics, data, audio, pictorial or other information representation in digital form that is created, modified, maintained, archived, retrieved or distributed by a computer system.

Electronic Signature: A computer data compilation of any symbol or series of symbols executed, adopted or authorized by an individual to be the legally binding equivalent of that individual's handwritten signature.

Digital Signature: An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

c. *Requirements*

Procedures and controls need to be put in place to ensure the authenticity, integrity and confidentiality of electronic records and ensure that signers cannot readily repudiate the signed record as not genuine. This requires that controls be put in place to manage records, control access to system and records, document changes to records and issuance and control of electronic signatures.

Systems are validated to ensure accuracy, reliability, consistent intended performance and to discern invalid or altered records.

- Information and electronic documents need to be managed in such a manner that information cannot be easily modified, obscured, obliterated or otherwise adulterated. Access to and ability to retrieve information must be maintained throughout the retention period. Electronic signatures must be associated with electronics records in a manner where it is difficult to remove or change the signature.
- Utilize audit trails that are operator independent, secure, computer generated and time-stamped. Record changes must not obscure or remove prior information. All changes made to records need to be documented with computer-generated records that identify the changes that were made, the author of the changes, time stamps of the changes and the reason for the changes. The ability to make changes must be limited to authorized individuals.
- Access to an automated system needs to be controlled and limited to only those authorized to access the system. Access to specific features and capabilities should be limited to those who have specific needs for them. For example, operators should not have access to system administration functions, but they should have access to features and capabilities required for them to perform their duties. Features required include:
  - Limiting access to authorized individuals
  - Using authority checks to ensure that only authorized individuals can use the system
  - Using of device checks to determine, as appropriate, the validity of the source of data input
  - Controlling distribution and access to systems documentation used for system operation and maintenance
- Automated systems need to be set-up so that electronic signatures are unique to an individual, cannot be repudiated or stolen and cannot be used by others. This requires that:
  - An electronic signature is unique to one individual and not reused by or reassigned to anyone else
  - Electronic and handwritten signatures executed to

electronic records shall be linked to their respective electronic records to ensure that they cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means

- Non-biometric signatures shall employ at least two distinct identification components, be used only by their genuine owners and not be disclosed to any unauthorized personnel. ID codes in combination with passwords require controls to ensure security and integrity. No two people can have the same ID/password combination.
- Manufacturers need to verify an individual's identity before an electronic signature is established or assigned

d. User Responsibilities

The first decision users need to make is whether or not they want or need to comply with 21CFR Part 11. Compliance to this regulation is voluntary, but if a manufacturer is creating, modifying, maintaining, archiving, retrieving or transmitting via computer systems any records with requirements set forth in agency regulations then those computer systems will need to comply with 21CFR Part 11.

Once users determine that they need or want to comply with 21CFR Part 11 then they need to perform the following:

- Audit existing systems to determine if: (1) they need to comply with Part 11, and (2) what is their present state of compliance. Perform a gap analysis similar to what was done for Y2K.
- Develop a Compliance Strategy Document to state their position and requirements to achieve Part 11 compliance.
- Put policies and SOPs in place for Part 11 compliance
- Assign a Part 11 compliance officer.
- Begin Part 11 compliance training to improve awareness.
- Clearly define intentions and strategy including:
- Security strategy including policy on use/dissemination of electronic signature
- What systems will be Part 11 compliant
- What is required for data integrity and audit trails
- Back-up, archive, and disaster-recovery strategies
- Prioritize activities based on drug safety, efficacy, and identity
- Include these requirements in your project validation plans and user requirement specifications as needed.

V. Compliance with Pro-Watch

a. 21CFR Section 11.10 (a)(b)

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Requirement	The system shall be validated with written procedures designed to assure that the drug products have the proper quality control sequences in place to ensure the integrity of the entire operation. These written procedures, including any changes, shall be drafted, reviewed and approved by the appropriate organizational units, then reviewed and approved by the quality control unit. These written procedures shall be documented at the time of performance. Any deviation from the written procedure shall be recorded and justified. The system shall be capable of generating accurate and complete copies of records to either paper or electronic media. Evidence of this capability should be apparent in the validation documentation. The agency requires that electronic records, electronic signatures and handwritten signatures executed to electronic records be trustworthy, reliable and generally equivalent to paper records and handwritten signatures executed on paper.
Compliance Statemen	Established procedures must ensure that system tests are being planned to cover items 11.10(a)(b). Testing activities must adhere to the principal of Good Testing Practices to enable proper step-by-step tracing of the tests, the test results and the responsible person(s) for each activity. Honeywell can assist the customer in establishing these testing procedures. Pro-Watch can be proven to adhere to these design intentions. Once installed, Site Acceptance Tests (witnessed by the customer) must be conducted to demonstrate that the system is correctly working within its dedicated environment for its intended purpose.
Remarks	Customer responsibility to develop the documents, maintain validation procedures and results. Honeywell can assist in this effort.

b. 21CFR Section 11.10 (c):

Protection of records to enable their accurate and ready retrieval throughout the record's retention period.

Requirement	1. A method of retaining records electronically throughout the necessary retention period shall be documented and proven.
Compliance Statement	Events are collected in the Pro-Watch database. Periodically, events are copied from the Pro-Watch database to file storage. This is done to keep the operating database a reasonable size. Events are archived then purged from the online storage according to a schedule you specify. The archive files are stored on the secure server and can be bought back into the operating database for reporting when needed. Alternatively, Honeywell Access Systems offers an optional Report/Archive Server. This report server can store events online ready for reporting. A database separate from Pro-Watch's operational

	DB is used as a data warehouse and record retention is limited only by the size of the data disks.
Remarks	Archiving allows you to archive events to the Pro-Watch server. These archives can then be moved to tape, CD or be included in the customer's corporate system backup program. Backup media must be legibly labeled with volume name and dates range, and media library stored in a safe and environmentally sound place.

Requirement	2. If the system is identified as the record storage location throughout the retention period, a capacity analysis should be performed to ensure that the system software and hardware can accommodate projected record volume.
Compliance Statement	A provided guideline and sample for calculating online storage capacity is available below. Use the same calculations for offline storage minus the base value.
Remarks	A base value* of 750 MB , plus 2000 bytes per event** of database space is required. To estimate the disk space required, the following information is needed: • An estimate of the events generated per day. • Number of day's events are to be kept online, readily available; for example – the system generates 1000 events per day and the events are to be kept online for 180 days. The disk space estimation for events would be: (1000 events * 180 days) * 2000 bytes = 360,000,000 bytes or 360 MB. Add the base value of 750 MB to the estimation above; you would require 1.11GB of database space. *This is only a sample, the base value changes according to system size and options. **An "event" is an Alarm Event, Card Read, or Operator Action.

Requirement	3. If system software, hardware or operating system upgrades are identified as the method of ensuring record "retrievability" throughout the retention period, test plans should be in place for data migration verification.
Compliance Statement	Pro-Watch has a Legacy Restore Utility that brings archives created from earlier versions into a format usable with the newer versions. This utility has not been needed since very early versions of Pro-Watch. Should this utility be needed again, Honeywell Access Systems will insure - no data from the archives will be altered - only the format in which it's stored.
Remarks	In Pro-Watch go to the administration section | executables | Legacy restore utility.

c. 21CFR Section 11.10 (d)

Limiting system access to authorized individuals

Requirement	System access should be limited to only authorized individuals
Compliance Statement	Pro-Watch used a combination of Windows authentication and Pro-Watch operator permissions assigned within the application. Security credentials (Usernames & passwords) are stored in Windows Active Directory. Permissions within the application are defined with Pro-Watch operator classes and at the individual operator level. These permission levels are very granular and can be adjusted as needed.
Remarks	Assigning a new operator works as follows: • A Windows account is created in Active Directory. • This user is typically added to a Windows Security Group • The user is then added to Pro-Watch and assigned an operator class. This operator class will have a set of permissions pertaining to different functions

	within the application. Classes and their associated permissions can be added and edited as needed by system administrators. If further granularity in permission setting is needed, it can be adjusted at the individual operator level.

Requirement	2. System testing shall include a verification of system access security - i.e. if the system employs “front-end” security, testing should verify that “back-end” entry would require system manipulation considered “beyond reasonable means.”
Compliance Statement	Pro-Watch workstation must be configured as a “secured workstation” to prevent accessing the operating system and software other than Pro-Watch applications software. A “secured workstation” works as follows: • Prevent operators from shutting down their computer • Prevent users from locking the computer • Remove access to applications via Task Manager and Windows • Automatic starts of Station upon successful logon to Windows
Remarks	**To prevent Shut Down By changing the local policies:** 1. Select *Start* > *Settings* > *Control Panel.* 2. Select *Administrative Tools*. 3. Select *Local Security Policy.* 4. Select *Local Policies* > *User Rights Assignment.* 5. Double-click *Shutdown the system*. The Local Security Policy Setting dialog box is displayed. 6. Click *Add*, select *Pro-Watch User,* click *Add*, click *OK.* 7. Deselect *Local Policy Setting* for *Pro-Watch User*, click *OK*. 8. Close *Local Security Settings*. **To Prevent Operator Shut Down By Editing The Registry:** 1. Select *Start* > *Run*, type *regedit* and click *OK*. The Registry Editor opens. Locate the key: *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\ CurrentVersion\Winlogon\ShutdownWithoutLogon* Set its value to *0*. Click *OK*. 2. Close *Registry Editor*. **To disable the Lock Computer option:** Temporarily assign Pro-Watch User as a member of the “Administrators” group to complete this procedure. 1. Select *Start* > *Settings* > *Control Panel.* 2. Select *Administrative Tools.* 3. Select *Computer Management*. 4. Select *Local Users and Groups* > *Users* 5. Double-click *Pro-Watch User,* select *Member of,* click *Add*. 6. Select *Administrators* > *Add* > *OK.* 7. Click *Apply*, click *Close*. **Disable The Lock Computer Option For Pro-Watch User**. 1. Log off as “*Administrator*”. 2. Log on as “*Pro-Watch User”.* 3. Select *Start* > *Run,* type *Regedit* and click *OK*. The Registry Editor opens. 4. Create or locate the key: *MyComputer\ HKEY_CURRENT_USER\ Software\ Microsoft\Windows\ CurrentVersion\Policies\System* 5. Add a new DWORD value DisableLockWorkstation (right-click, click *New*, select *DWORD Value*, name the new DWORD *DisableLockWorkstation*). Set the value to 1 to disable Lock Workstation.

6. Exit the *Registry Editor*.
Note:
To disable the *Task List* Option & *Lock Workstation* buttons in the <Ctrl>+<Alt>+<Del> screen, repeat step 5 and add the new DWORD's *DisableTaskMgr* and *DisableLockWorkstation*. Set the value to 1 for each key.
After this procedure has been completed, remove Pro-Watch User as a member of the "Administrators" group.
1. Log off as "*Pro-Watch User*"
2. Log on as "*Administrator*"
3. Select *Start > Settings > Control Panel*
4. Select *Administrative Tools*
5. Select *Computer Management*
6. Select *Local Users and Groups > Users*
7. Double-click *Pro-Watch User*, select *Member of*
8. Select *Administrators > Remove > Apply > Close*
9. Close *Computer Management*.
To Remove Access To Task Manager And Windows Explorer:
1. In Windows Explorer, right-click the file *winnt\system32\taskmgr.exe*.
2. Select *Properties > Security*
3. Click *Add*
4. Select the users you want to modify (e.g. *Pro-Watch User*), click *Add*, click *OK*
5. Select the user you added, click *Deny* for *Full Control*.
6. Click *Apply*, click *OK*
7. Select *Yes* in response to the "Do you wish to continue?" prompt
8. Repeat steps 1 through 7 of this task for the file *\winnt\explorer.exe.*

Creating a Batch File to Start Station

In order for operators to access Station on a secure computer, you need create a batch file that enables Station to start automatically when the operator logs on to the computer.

Specifying the Batch File as a Logon Script

Once you have created the batch file, you need to associate the batch file with the "Pro-Watch User" account so that the batch file runs when an Pro-Watch operator logs on.
To specify the batch file as a logon script::
1. Select *Start > Settings > Control Panel.*
2. Select *Administrative Tools.*
3. Select *Computer Management*.
4. Select *Local Users and Groups > Users*.
5. Double-click on the account "Pro-Watch User". The *Properties* dialog box is displayed.
6. Select *Password never expires*.
7. Click *Apply*.
8. Click *Profile* and in the *Logon Script* field, "batfile name"
9. Click *Apply*, click *Close* to close the *Properties* dialog box.
10. Close Computer Management

Requirement	3. The system shall allow for the maintenance of historical user access lists.
Compliance Statement	Pro-Watch system events, such as operator login/logout are written to the event table, where it can be accessed for reports or displays on a Station. The event

	table is achieved to a flat file as the on-line storage becomes full. In addition, Windows NT/2K Security log also records security events such as valid and invalid logon attempts.
Remarks	Windows log on auditing must be enabled to record the log on attempts in the security log. By default, security logging is turned off. You can use Group Policy to enable security logging. The administrator can also set auditing policies in the registry that cause the system to halt when the security log is full. Better yet, third party tools can save logs in file form when the log reaches it's limits

Requirement	4. If the system allows for different classifications of operators, the system should enforce constraints defined in the user definition (i.e. if the system allows for different permissions for system administrator level access and system user access, these permissions should be enforced. System testing should verify these constraints
Compliance Statement	• Hardware, alarm / event routing and other configuration elements may be partitioned • Operators can be assigned access to one or more particular partition(s) • Operators can be authorized to access only selected workstations. In addition, they may be authorized for only selected days of the week and even hours of the day. • The security level that has been assigned to each operator limits access to Pro-Watch functions • Pro-Watch has unlimited security levels (Classes) • An operator is assigned a Class and may only perform functions assigned to them
Remarks	Operator classes are totally configurable and should be tested before assigning operators.

d. *21CFR Section 11.10 (e)*

Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Requirement	1. The system shall include automatic, secure audit trails. 2. Audit trails shall include the operator ID. 3. Audit trails shall include a date and time stamp. 4. Operators shall not have access to the source of the date/time parameters.
Compliance Statement	Operator ID, operator name, date and time are captured in the Audit/Event tables. The table contents cannot be altered or deleted without extraordinary means.
Remarks	Operator must not be assigned with Windows administrator privileges or SQL SA privileges. An SQL role shall limit access to these tables. Also, Only Windows administrators will have access to date/time setup parameters. See this document for procedures on how to setup a "secured workstation".

Requirement	5. Time stamp shall be local time.
Compliance Statement	Pro-Watch logs server's local time as "recorded event time" in EV_LOG and also logs the local time the event happened in the field .

Remarks	Pro-Watch records the time the server records the event and the time the event happened in the field. This is important for accuracy across time zones

Requirement	6. Audit trails shall mark all operator entries or actions which create, modify or delete electronic records.
Compliance Statement	All operator activities, like device adjustments, Access changes and alarm acknowledgements are recorded in the Event Log. Installer activities like adding points, deleting points and modifying points are also recorded in the Event Log. Recorded events include the name of the operator responsible for the action, the date, time and reason the before value and after value. These events can be viewed in the Audit Log Report.
Remarks	This log cannot be modified or deleted.

Requirement	7. Record changes shall not obscure previously recorded information.
Compliance Statement	The Event Log is used to provide audit trail. i.e. when a device parameter is changed, the original value and the new value are recorded in the event log.
Remarks	The Pro-Watch pre-configured report enables you to query the audit log to provide a picture of what occurs to a specific point. The report would have the actual value of the pre- and post-change, the exact time and date, the reason for the change and who made the change.

Requirement	8. Audit trails shall be retained throughout the retention period. 9. The system shall be capable of generating accurate and complete copies of the audit trail to either paper or electronic media.
Compliance Statement	Pro-Watch system stores the audit trail in an Event Log, where it can be accessed for reports. The event log can be archived to a tape library (or other removable media) as the on-line storage becomes full. There is no limit to the number of tape or other types archives.
Remarks	Pro-Watch system stores the audit trail in an audit log, where it can be accessed for reports. The audit log can be archived to a tape library (or other removable media) as the on-line storage becomes full. There is no limit to the number of tape or other types archives.

Requirement	10. System testing shall include a verification of audit trail security, i.e. controls should be in place so that audit trail manipulation would require actions, which are “beyond reasonable means.” Testing should verify the robustness of these controls.
Compliance Statement	Pro-Watch database, tables and history archive files are not available in the human-readable form. In addition, access of the database tables and archive files should be controlled with SQL permissions and Windows file level permissions attributes.
Remarks	The files and folders in Windows 2000/2003 have property sheets that display information about the file or folder, such as the size, location and the date it was created. When you view the properties of a file or folder, you can also get information about the file or folder attributes. The Security tab lists other users who can modify, read and execute, list folder contents, write to the file or folder, or have read-only access.

e. 21CFR Section 11.10 (f)

Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Requirement	1. System logic should be designed so as to ensure permitted sequencing of steps and events. 2. System testing shall include verification that operational steps are enforced.
Compliance Statement	Pro-Watch provides multi-stage alarm management and operator response management to help operators respond appropriately to alarms and provides a way for operators to record their responses to alarms.
Remarks	Pro-Watch provides a choice of many advanced alarm management methods i.e. forcing an operator response to particular event types, predefined responses and HTML detailed instruction

f. 21CFR Section 11.10(g)

Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Requirement	1. System shall employ authority checks to ensure that only authorized individuals can use the system. 2. System test shall include authority checks on electronically signing of record. 3. System test shall include authority checks on accessing the system. 4. System test shall include authority checks on operating the system. 5. System test shall include authority checks on alteration of record. 6. System test shall include authority checks on performing the operation at hand.
Compliance Statement	• Pro-Watch employs Windows Authentication and SQL Security roles for access to the application, database and files. • Certain operators can be designated as signers . • In addition to application, a system modification can be configured to require single or double signatures as well as a reason for the action.
Remarks	Pro-Watch uses a unique feature that can be assigned to any channel and it's associated child objects. When this feature is enabled for a channel, Pro-Watch will required the operator to provide reason for change along with single or double signatures in order to change any parameter's value. • When a double signature is configured for channel, it will require two different operators with proper authorization to perform the point value change.

g. 21CFR Section 11.10(h)

Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Requirement	The system shall employ device checks, as appropriate, to ensure the validity of the source of data input, i.e. if the system is receiving data from multiple sources, it may be necessary to employ source identification verification.
Compliance Statement	Several types of checks are built into Pro-Watch, including authority checks that determine who has access to the system and at what level; and device checks

	that determine the validity of the sources of data being entered into the system.
Remarks	For added security, each Pro-Watch workstation and each operator may be configured to limit access to particular Pro-Watch partitions.

h. 21CFR Section 11.10 (i)

Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Requirement	Provides documented proof that the person who develops, maintains, or uses the system must have the education, training and experience to perform their assigned tasks.
Compliance Statement	Not Applicable to Pro-Watch. Pro-Watch provides ways to ensure only qualified personnel can access the system. Operators are assigned with access time, workstation stations, operator class, permissions and partitions which limit the operators to the area of the application on which they are trained.
Remarks	Customers are responsible for ensuring that all persons involved with regulated system have the necessary levels of education, training and experience to perform their assigned tasks. Customers are also responsible to maintain appropriate training documents. Honeywell can assist in providing system training and qualifying personnel.

i. 21CFR Section 11.10 (j)

The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Requirement	Establish written policies that hold individual accountable for actions initiated under their electronic signatures.
Compliance Statement	Not Applicable to Pro-Watch. Generally covered with SOP.
Remarks	Customer responsibility to develop and enforce policies and procedures to meet the regulations.

j. 21CFR Section 11.10 (k)

Use of appropriate controls over systems documentation including:
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Requirement	1. Controls over document distribution, access and use shall be employed.
Compliance Statement	Access of the help files and theory of operations documents can be controlled with Windows file property security attributes, however, if a person is granted access right to a document, there is no built-in mechanism to detect and prevent unauthorized copying and distributing of said document.
Remarks	Customer responsible to develop and enforce policies governing copying and distributing of document.

Requirement	2. Revision and change control procedures to maintain an audit trail.
Compliance	Any change to the Pro-Watch attributes for a designated set of hardware is

Statement	recorded in the event file. Installer activities like adding point, deleting point and modifying point are also recorded in the Event/Audit/Operator Logs.
Remarks	Access to database tools like MS Access, SQL Enterprise Manager and any other database manipulation tools must to be controlled to maintain audit trail. This may require "Pro-Watch only" designated workstations for system users.

ADDITIONAL REQUIREMENT FOR OPEN SYSTEMS

k. 21CFR Section 11.30

Controls for open systems

Persons who use open systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures, such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity and confidentiality.

Requirement	1. Records shall be encrypted to ensure authenticity, integrity and confidentiality 2. System testing shall include a verification of record security such that unauthorized reading and/or changing of records would require actions which are "beyond reasonable means"
Compliance Statement	Pro-Watch is classified as "closed system".
Remarks	Access of the files should be controlled with Windows file property security attributes. The files property sheets display information about the file attributes. The Security tab lists other users who can modify, read and execute, write to the file or have read-only access.

ELECTRONIC AND PAPER SIGNATURE REQUIREMENTS

l. 21CFR Section 11.50

(*a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:(1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.*

Requirement	(1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
Compliance Statement	Both the operator's ID and full name are printed with all operator events. Date/time, operator action, operator's ID, operator's name and meaning of An Operator's actions are recorded to the event log in such a way that they

	become part of the record.
Remarks	The Operator's ID and full name are defined in the Windows operating system. The System must be setup with an integrated account that is a combination of a Windows user account and a Pro-Watch operator definition. It is assumed that "meaning" refers to "reason for operator actions". Pro-Watch will prompt the user to select a reason for his/her action from a pre-configured list , free text can also be added.

m. 21CFR Section 11.50

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Requirement	This signature manifestation shall be present on all paper and electronic copies of the signed record, i.e. the signature shall be visible on both the screens, when viewing the record electronically and on the printouts, when viewing the record on paper.
Compliance Statement	Reports can be printed or displayed on an Operator workstation. Operator ID does not apply to all reports, but when the field is visible on the workstation screen it will also appear on the printed report.
Remarks	When viewing the record on screen, or printing the record on paper, the information is retrieved from the same server database. When a report is generated, the printout will look exactly as it appeared on the station screen.

n. 21CFR Section 11.70

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied or otherwise transferred to falsify an electronic record by ordinary means.

Requirement	1. Signatures shall be linked to their respective electronic records. 2. System testing should include a verification of signature/record linking robustness. 3. Signatures shall not be deleted, copied or transferred by ordinary means.
Compliance Statement	Operator ID and Operator Name are recorded to the event log in such a way that they become part of the record, i.e. each event is a record within the event log.
Remarks	The "Signature" is taken to mean operator ID and name.

GENERAL ELECTRONIC SIGNATURE REQUIREMENTS (Subpart C – Electronic Signatures)

o. 21CFR Section 11.100

***(a)** Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

Requirement	1. The system shall be designed so as to ensure that each electronic signature is unique and cannot be reassigned to anyone else. 2. System testing should include verification that any attempt to reassign electronic signatures or to duplicate electronic signatures will fail.
Compliance Statement	Pro-Watch is integrated to Windows user account management for operator assignment. Windows enforces that each operator has a unique ID and

	duplication of operator ID assignment is not allowed.
Remarks	Customer must develop SOP which details that system administrators are only to deactivate and not remove operators once they have been set up in the system.

p. *21CFR Section 11.100*

(b) Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

Requirement	The organization shall verify the identity of individuals before assigning electronic signatures. Pro-Watch is integrated to Windows user account management for operator assignment. Windows enforces that each operator has a unique ID and duplication of operator ID assignment does not occur.
Compliance Statement	Not applicable to Pro-Watch.
Remarks	Customer responsibility to develop and enforce policies to ensure positive identification of individuals before issuing the ID and password.

q. *21CFR Section 11.100*

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

> *(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.*
>
> *(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.*

Requirement	1. The organization shall submit a certification letter to the FDA. 2. The organization shall ensure that persons using electronic signatures have the education and training to provide additional testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.
Compliance Statement	1. Not applicable to Pro-Watch. 2. Every time an electronic signature is required to execute a specific task, a legal text is also displayed informing the operator that their electronic signature is the legally binding equivalent of their handwritten signature. The legal text displayed in the dialog box can be customized to your site's requirements.
Remarks	1. Customers are responsible for certifying to the agency that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures. The certification must be submitted in paper form and signed with a traditional handwritten signature. 2.Because of the legal liability associated with an electronic signature, an operator must unequivocally know whenever they are signing a record. Customers' responsibility to ensure that all employees involved with regulated system have the necessary levels of education and training to perform their assigned tasks.

NON-BIOMETRICS SIGNATURE REQUIREMENTS

r. *21CFR Section 11.200*

Electronic signature components and controls

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components, such as an identification code and password.

Requirement	1. Signatures shall employ two distinct identification components
Compliance Statement	Operator ID and Operator password are the two required components.
Remarks	The operator ID and password are configured in Windows user account management.

s. *21CFR Section 11.200*

(1) (i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

Requirement	(1)(i). When a series of signings are executed during a single, continuous period of controlled system access, the first signature shall include both components and subsequent signatures may include only one. (1)(ii). When a series of signings are not executed during a single, continuous period of controlled system access, all signatures shall include both components.
Compliance Statement	Pro-Watch requires an operator ID and password to initially sign-on to the station. Subsequent operator activities may require the re-entering of a valid password before that action is authorized. Any channel and its child objects can be configured to require a reason for change along with single or double signature as a reason for the action.
Remarks	1. When a user edits a device or issued a clearance code, a popup window appears on the station displaying the Primary Signature page of the Electronic Signature. A legal text is also displayed on the bottom part of the screen informing the user that their electronic signature is the legally binding equivalent of their handwritten signature. 2. At this time, the user may select one of the pre-defined reasons from a pull down window. 3. The user must supply the password and click on the “sign” button. The supplied password will then be authenticated. • For points configured with single signature, the command is executed if the password is valid. The event is recorded in the event log. • If the password is not valid, a warning message is raised on the workstation.

	4. For points configured with double signatures, the Second Signature page is displayed upon a valid entry of primary signature. 5. A second user must supply the password and click on the “sign” button. The supplied password will then be authenticated.

t. 21CFR Section 11.200

(a) (2) Be used only by their genuine owners; and
(3) Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Requirement	(2) Signatures shall be used only by their genuine owners. Controls should be in place to ensure that super users, such as system administrators and data base administrators, cannot use individual’s signatures. System testing should include a verification of this security. (3) Signatures shall be administered to ensure that the attempted forgery of an individual’s electronic signature requires collaboration of two or more individuals.
Compliance Statement	When an operator or system administrator logs on to the system, all actions taken under that login is signed as that person’s ID. A system administrator is unable to log on as another user without their password, which is encrypted and not readable. The operator ID and password are configured in Windows user account management. A system administrator alone is able to setup and configure operators. It does not require two persons to administer an operator.
Remarks	To attempt to log on as a different user, a system administrator must first issue a new password for that user; this will require a second manager level person’s collaboration to accomplish. This action is recorded in the event log. It is the customer’s responsibility to develop and enforce policies and procedures to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals. For example, the Pro-Watch system administrator is required to secure his/her supervisor approval in writing before carrying out the task of operator configuration.

BIOMETRICS SIGNATURE REQUIREMENTS

u. 21CFR Section 11.200

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Requirement	Signatures which employ a measurement of the individual’s physical feature(s) or repeatable action(s) shall be designed to ensure that they cannot be used by anyone other than their genuine users (system testing shall include a verification of biometrics signature security).
Compliance Statement	Pro-Watch does not directly employ any biometric signature logging into the application. If a biometric login is used for accessing operating system this login procedure should conform to a windows authentication method and will be considered the same as a standard windows login.
Remarks	A biometric login to the operating system will be considered the same as a standard windows login when considering the Audit trail

REQUIREMENTS FOR NON-BIOMETRICS SIGNATURES WHICH ARE IMPLEMENTED BY THE USE OF IDENTIFICATION CODE/PASSWORD COMBINATIONS

v. 21CFR Section 11.300

Controls for identification codes/passwords

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Requirement	(a) 1. The uniqueness of the ID/Password combinations shall be enforced.
Compliance Statement	Pro-Watch is integrated to Windows user account management for operator assignment. Attempts to assign an ID that has already existed in the system are rejected by Windows.
Remarks	Pro-Watch follows the model set forth by the Windows operating system, including all features and limitations like user name and password length.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (i.e. to cover such events as password aging).

Requirement	(b) 1. The system shall include automatic passwords expiration
Compliance Statement	Operator passwords will expire after the user specified number of days and a new password will be required.
Remarks	The Windows password validation period feature is configurable. If activated, it will not allow operators to re-use a password that has already been used during the configured period. For example, you may configure the system to impede users from re-using the same password for 60 or 365 days.

(c) Following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

Requirement	(c) 1. Loss management procedures shall be in place. (c) 2. The system shall allow for the electronic de-authorization of passwords.
Compliance Statement	Passwords can be configured to expire periodically e.g. every 60 days.
Remarks	Customer to establish loss management procedures. Implement redundant server architecture if necessary to minimize risk of system failure.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Requirement	(d) 1. The system shall automatically log signature attempt failures. (d) 2. This log should be readily available for review. (d) 3. This log should be monitored by system administrators. (d) 4. The system should alert administrators of multiple signature failures.
Compliance Statement	Unsuccessful login attempts are detailed as alarm events and recorded in the Operating system's event log.
Remarks	After a specified number of unsuccessful login attempts, the Operator workstation is a lockout (i.e. will not accept keyboard inputs). It will stay locked out for a period of time specified by the user.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manor.

Requirement	(e) 1. If the ID or password is generated by a device, the device should be initially and periodically tested to ensure that the device is functioning properly and has not been altered in an unauthorized manner.
Compliance Statement	Pro-Watch does not use any device to generate ID or password.
Remarks	Not applicable to Pro-Watch.

VI. Services

As security management systems continue to become part of globally managed security networks, it has become clear that professional services, such as global project management, applications engineering and electronic documentation, are required by our customers. End-users of Honeywell Access Systems (HAS) across the globe have requested that HAS, as the Manufacturer, provide these professional services directly to assure that these systems are a coordinated effort where multiple contractors/vendors are utilized. This allows the end-user to select the best local service providers globally and have them be a part of a coordinated effort by Honeywell to assure scope, schedule and budget, as well as meet special Regulatory requirements. The HAS Professional Services Group was formed to address these critical project requirements and ensure that these unique projects realize their full potential.

This professional services document includes elements that take a proactive approach to a global security management installation at all phases of the project. This document provides our customers with the peace-of-mind that all aspects of a global security management system project are considered and mapped out in a critical process environment. This document also provides definition to some of Honeywell's additional value added services.

This section discusses how Honeywell systems and services can assist clients specifically with project validation – for a complete view of all services offered by Honeywell please see the Professional Services in a Validated Environment document. The intent of this document is to provide a broad view of the required elements for supporting system validation to the Pharmaceutical regulated industry. As no two projects are identical, detailed responses are supported on a per project basis as part of the functional specification.

a. Overview of Validation Consulting Services

As the industry's most seasoned provider of *Conformance and Validation Services*, Honeywell can help you reduce the risk of non-compliance at regulated sites, and in doing so, avoid fines and recalls imposed under FDA and other guidelines. No other automation provider has as many field service resources or as much industry experience and technical expertise in crafting a client-specific, cost-effective solution for maintaining compliance.

Honeywell's best-in-class validation solution for environmental systems helps customers document that their automation systems perform as expected in compliance with the FDA's cGMP standard, including 21CFR Part 11.

Our cGMP-trained technicians can also provide validation assistance for other aspects of your manufacturing operation and help with creation of a thorough validation plan. In addition, they can assist with the preparation and execution of Installation Qualification (IQ), Operation Qualification (OQ) and Performance Qualification (PQ) protocols and perform the on-going calibration and maintenance work required to maintain your equipment in its validated state.

b. User Responsibilities

In order for Honeywell's services to be effective, the user must make a commitment to compliance. While Honeywell is supporting the user, the user will also have responsibilities. The first decision users need to make is whether or not they want or need to comply with 21CFR Part 11. Compliance to this regulation is voluntary, but if a manufacturer is creating, modifying, maintaining, archiving, retrieving or transmitting via computer systems any records with requirements set forth in agency regulations, then those computer systems will need to comply with 21CFR Part 11.

Once users determine that they need or want to comply with 21CFR Part 11, they need to do the following:

- Audit existing systems to determine if: (a) they need to comply with Part 11, and (b) what is their present state of compliance.
- Perform a gap analysis similar to what was done for Y2K.

- Develop a Compliance Strategy Document to state their position and requirements to achieve Part 11 compliance.
- Put policies and SOPs in place for Part 11 compliance.
- Assign a Part 11 compliance officer.
- Begin Part 11 compliance training to improve awareness.
- Clearly define intentions and strategy including: security strategy – including policy on use/dissemination of electronic signature; what systems will be Part 11 compliant; what is required for data integrity and audit trails
- Back-up, archive, and disaster-recovery strategies
- Prioritize activities based on drug safety, efficacy and identity
- Include these requirements in your project validation plans and user requirement specifications as needed.

c. *Project Services*

To assist in project execution, Honeywell can prepare and execute protocols required for system validation.

Honeywell can prepare Validation Protocols – a written plan of the activities required to validate the control system under consideration. The Validation Protocol would include:

1) An overview of the validation project
   - The objective of validation
   - An explanation of the validation process
   - Identification of the personnel responsible for designing validation
   - Identification of the Validation Core Team and their responsibilities
   - An explanation of Validation Protocol Approvals
   - An explanation of the Project Change Control Procedure

2) The Control System Definition:
   - Pro-Watch system Hardware Specifications with Drawings
3) An explanation of the Validation Project Segments:
   - Design Qualification
   - Installation Qualification
   - Operational Qualification
   - Performance Qualification

4) Validation Project Responsibilities

5) Validation Project Deliverables

Shortly after the final approval of the Validation Protocol, Honeywell can provide the customer with an Installation Qualification Protocol.

This Protocol is a set of objectives outlining criteria that must be met, procedures that must be followed and technical records that must be completed in order to ensure that the Honeywell Control System, as submitted per the System Specification, has been installed in accordance with the manufacturer's recommendations. Installation Qualification Protocol objectives address the following areas:

- Assess Physical Placement of the Control System
- Assess Control System Grounding
- Equipment Inventory and Installation
- Assess Computer System Cable Installation
- Assess Control System AC Power Source and RFI
- Power-On Checks
- Hardware Modules Self-Tests
- Execution of Diagnostic Test Programs
- Software Inventory and Installation
- Verification of Normal Equipment Power Up/Power Down
- Installation of Custom Programs (custom graphics, reports, programs)
- Backup and Recovery of Software
- Backup and Recovery of Redundant Modules
- Identification of User and Support Personnel Requirements (by the customer)
- Identification and Assessment of Appropriate SOP's (by the customer)
- Inventory and Assessment of Documentation (by the customer)
- Assessment of the System Security (by the customer)
- Identification of Hardware and Software Maintenance Support (by the customer)
- Location and Identification of Spare Parts (by the customer)

During approval of the Installation Qualification Protocol, the project team, client and Honeywell will identify the tasks to be performed by Honeywell.

After submittal of the Installation Qualification Protocol, Honeywell can provide the customer with an Operational Qualification Protocol. The Operational Protocol is a set of objectives with criteria that must be met, procedures that must be followed and forms that must be completed in order to ensure that the Control System operates throughout representative or anticipated ranges as intended in the System Specification submitted to Honeywell. Operational Qualification Protocol Objectives address the following areas:

- System Startup and Shutdown
- System Access Security (performed by the customer)

- System Special Diagnostic Software
- Automatic Fail-over
- Alarms and Enunciators
- Discrete Input and Output loops
- Analog Input and Output Loops
- Control Loops
- Logic
- Custom Graphics
- Custom Application Programs
- Custom Reports

During approval of the Operational Qualification Protocol, the project team, client and Honeywell will identify the tasks to be performed by Honeywell.

If asked to perform these services, Honeywell has completed its validation services when a complete set of approved protocols, a completed set of Installation Qualification technical records are filed for all identified equipment and a completed set of Operational Qualification technical records are filed for all identified hardware and software. One set of these documents will be provided and Honeywell will refer to this documentation as Comprehensive Technical Records.