

 <p>Biotechnology Regulatory Services</p>	<b>Animal and Plant Health Inspection Service</b> <b>Biotechnology Regulatory Services</b>	Document Control #: <b>1000AppendixA</b> Version: <b>1.0</b>
<b>APHIS BQMS PROGRAM GENERAL ADMINISTRATIVE PROCEDURE APPENDIX A: HANDLING CONFIDENTIAL BUSINESS INFORMATION</b>		<b>Effective Date: 093010</b>

## 1. PURPOSE

This document outlines the responsibilities and requirements for all Animal and Plant Health Inspection Service (APHIS) Biotechnology Quality Management System Program (BQMS Program) officials, including agents of APHIS, such as third-party auditors, for the handling of material considered Confidential Business Information (CBI).

Documents may be justified as containing CBI by participants of the APHIS BQMS Program and are entitled to treatment as trade secret or proprietary data.

Participants of the APHIS BQMS Program may seek voluntary verification of their implemented and established Biotechnology Quality Management System. Procedural requirements of this verification process may require handling of CBI by APHIS BQMS officials and third-party auditors. APHIS BQMS officials may require a desk audit review of a participant's documents containing CBI (i.e., documented procedures, work instructions, checklists, forms, etc.).

APHIS BQMS officials store CBI documents using the APHIS secure network, provided the following conditions are met:

- a. Files containing CBI must have the document naming standard “\_cbi” at the end of the file name. This includes files which are received as electronic files as well as paper documents which are scanned and saved electronically.
- b. Files containing CBI must be password-protected, so that a password is required to open the file.
- c. If a file containing CBI is sent via email, it may only be sent to APHIS email addresses and each email must be sent on the CBI disclaimer stationary.
- d. When sending a CBI document by email, APHIS BQMS Program officials must be connected directly to the APHIS network or signed into the Virtual Private Network (VPN) Client to secure the required firewall.

APHIS BQMS Program officials may transfer CBI documents to third-party auditors for a desk audit (stage 1 audit) as described in Section 8 of *1000\_BQMS\_General Administrative Procedure*, provided the following conditions are met:

- a. Files containing CBI must have a “red-jacket” indicating the documents contain CBI.

Examples of documents that may be received and/or retained by the APHIS BQMS Program that may be considered CBI justified by a participant may include, but are not limited to:

 <p>Biotechnology Regulatory Services</p>	<b>Animal and Plant Health Inspection Service</b> <b>Biotechnology Regulatory Services</b>	Document Control #: <b>1000AppendixA</b> Version: <b>1.0</b>
<b>APHIS BQMS PROGRAM GENERAL ADMINISTRATIVE PROCEDURE APPENDIX A: HANDLING CONFIDENTIAL BUSINESS INFORMATION</b>		<b>Effective Date: 093010</b>

- BQMS Quality Manual
- Documented procedures, work instructions, standard operating procedures, checklists, forms
- BQMS audit report

## 2. SCOPE

In accordance with *Federal Register* notice 50 FR 38561 (Monday, September 23, 1985) APHIS Policy Statement on the Protection of Privileged or Confidential Business Information, documents submitted to or created by the APHIS BQMS Program and containing CBI must be protected from unauthorized disclosure.

Any documents containing CBI, whether received electronically or on paper, must be handled in accordance with these procedures.

## 3. DEFINITIONS

*Confidential Business Information*—is abbreviated as CBI

*Document Warehouse*—a system of electronic folders on a secure network drive at (I://BRS/Biotechnology Regulatory Services/Document Warehouse). The secure folders within the secure network drive may be accessed only by APHIS BQMS Program staff.

*CBI training*—annual course which must be completed by all individuals who have a need to handle CBI.

*Disclaimer statements*—text attached to each email containing CBI, indicating the contents of the email and the responsibilities of the recipient.

## 4. RESPONSIBILITIES

Any APHIS BQMS Program official who receives or creates a CBI document must follow the procedure below. Everyone handling CBI must continue to renew their APHIS BRS CBI training annually and handle the information securely.

This CBI procedure also applies to BQMS Program Review Committee members and third-party auditors.

 <p>Biotechnology Regulatory Services</p>	<b>Animal and Plant Health Inspection Service</b> <b>Biotechnology Regulatory Services</b>	Document Control #: <b>1000AppendixA</b> Version: <b>1.0</b>
<b>APHIS BQMS PROGRAM GENERAL ADMINISTRATIVE PROCEDURE APPENDIX A: HANDLING CONFIDENTIAL BUSINESS INFORMATION</b>		<b>Effective Date: 093010</b>

## 5. PROCEDURES

### 5.1 Electronic Handling of CBI

CBI may only be sent to APHIS BQMS Program officials who have completed their annual CBI training. Lists of trained staff are maintained in the APHIS BRS secure network drive.

If a paper document containing CBI is received by APHIS BQMS officials, it may be scanned and saved to the APHIS BRS secure network drive in the appropriate folder.

If an electronic file (.doc, .xls, .pdf, etc.) is received or created by APHIS BQMS Program officials, it may be saved to the APHIS BRS secure network drive in the appropriate folder. The document naming standard must be used to name the file and in addition, “\_cbi” must be included at the end of every file name.

All electronic CBI documents must be password protected. All CBI-trained APHIS BQMS Program officials who require access to electronic CBI files will receive a password from the APHIS BQMS Program.

All emails (whether they contain CBI or not) must contain the following statement in their signature: **“CONFIDENTIALITY NOTE: This message is intended only for the named recipient and may contain confidential, proprietary or legally privileged information. Unauthorized individuals or entities are not permitted access to this information. Any unauthorized dissemination, distribution, or copying of this information is strictly prohibited. If you have received this message in error, please advise the sender by reply email, and delete this message and any attachments. Thank you.”**

Additionally, all CBI documents sent by email must be sent using the disclaimer statement stationery. The following text must be included in the stationery: **“NOTICE: This email may contain information that must be treated as trade secret or proprietary data under Section (b) (4) of the Freedom of Information Act (FOIA) {5 U.S.C. 522 (b) (4)}. Any person transmitting/handling or using the attached data in any way is responsible for preventing unauthorized disclosure during possession and must have completed the annual training for handling confidential business information. This information is not to be published, reproduced, publicly discussed, included in response to a FOIA request, or otherwise released without the explicit written authorization of the appropriate division director or designee. If you are not connected directly to an APHIS network, you must first sign into the VPN Client before logging into Lotus Notes to secure the required firewall.”**



 <p>Biotechnology Regulatory Services</p>	<p align="center"><b>Animal and Plant Health Inspection Service</b> <b>Biotechnology Regulatory Services</b></p>	<p>Document Control #: <b>1000AppendixA</b> Version: <b>1.0</b></p>
<p><b>APHIS BQMS PROGRAM GENERAL ADMINISTRATIVE PROCEDURE APPENDIX A: HANDLING CONFIDENTIAL BUSINESS INFORMATION</b></p>		<p><b>Effective Date: 093010</b></p>

CBI may only be sent to email addresses ending in “@aphis.usda.gov”.

CBI may not be saved to the computer hard drive. The hard drive can be stolen and is not backed up automatically. CBI documents can only be saved to the APHIS BRS secure network drive, which are backed up and secured.

Electronic CBI documents may be destroyed by permanent deletion off the secure network drive.

## **5.2 Hardcopy Distribution of CBI**

CBI may only be sent to APHIS BQMS officials, Program Review Committee members, and third-party auditors who have completed their annual CBI training. Lists of trained staff are maintained in the Document Warehouse.

Hard copies *must* be accompanied by a “red jacket” which indicates the file contains CBI and is protected under Section (b)(4) of the Freedom of Information Act (FOIA) {5 U.S.C. 552(b)(4)}.

Any person handling the files containing CBI is responsible for preventing unauthorized disclosure during possession.

Any person handling the files containing CBI must maintain the document under secure conditions.

Any person handling the files containing CBI must return the files back to the APHIS BQMS Program after use.

The BQMS Program is responsible for disposal and disposition of the files containing CBI. Files may either be shredded or returned to the BQMS Program participant.