ANNEX 4: COMPUTERIZED SYSTEMS

Section 1.01 Principle

The introduction of computerized systems into systems of manufacturing, including storage, distribution and quality control does not alter the need to observe the relevant principles given elsewhere in the Guide. Where a computerized system replaces a manual operation, there should be no resultant decrease in product quality or quality assurance. Consideration should be given to the risk of losing aspects of the previous system by reducing the involvement of operators.

Section 1.02 Personnel

1. It is essential that there is the closest co-operation between key personnel and those involved with computer systems. Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilizes computers. This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerized system.

Section 1.03 Validation

2. The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether it is prospective or retrospective and whether or not novel elements are incorporated. Validation should be considered as part of the complete life cycle of a computer system. This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and changing.

Section 1.04 System

3. Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.

4. A written detailed description of the system should be produced (including

ANNEX 4: COMPUTERIZED SYSTEMS

diagrams as appropriate) and kept up to date. It should describe the principles, objectives, security measures and scope of the system and the main features of the way in which the computer is used and how it interacts with other systems and procedures.

5. The software is a critical component of a computerized system. The user of such software should take all reasonable steps to ensure that it has been produced in accordance with a system of Quality Assurance.

6. The system should include, where appropriate, built-in checks of the correct entry and processing of data.

7. Before a system using a computer is brought into use, it should be thoroughly tested and confirmed as being capable of achieving the desired results. If a manual system is being replaced, the two should be run in parallel for a time, as part of this testing and validation.

8. Data should only be entered or amended by persons authorized to do so. Suitable methods of deterring unauthorized entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. There should be a defined procedure for the issue, cancellation, and alteration of authorization to enter and amend data, including the changing of personal passwords. Consideration should be given to systems allowing for recording of attempts to access by unauthorized persons.

9. When critical data are being entered manually (for example the weight and batch number of an ingredient during dispensing), there should be an additional check on the accuracy of the record which is made. This check may be done by a second operator or by validated electronic means.

10. The system should record the identity of operators entering or confirming critical data. Authority to amend entered data should be restricted to nominated persons. Any alteration to an entry of critical data should be authorized and recorded with the reason for the change. Consideration should be given to the system creating a complete record of all entries and amendments (an "audit trail").

ANNEX 4: COMPUTERIZED SYSTEMS

11. Alterations to a system or to a computer program should only be made in accordance with a defined procedure which should include provision for validating, checking, approving and implementing the change. Such an alteration should only be implemented with the agreement of the person responsible for the part of the system concerned, and the alteration should be recorded. Every significant modification should be validated.

12. For quality auditing purposes, it should be possible to obtain meaningful printed copies of electronically stored data.

13. Data should be secured by physical or electronic means against willful or accidental damage, and this in accordance with item 5.8 of the Guide. Stored data should be checked for accessibility, durability and accuracy. If changes are proposed to the computer equipment or its programs, the above-mentioned checks should be performed at a frequency appropriate to the storage medium being used.

14. Data should be protected by backing-up at regular intervals. Back-up data should be stored as long as necessary at a separate and secure location.

15. There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. For example, information required to effect a recall must be available at short notice.

16. The procedures to be followed if the system fails or breaks down should be defined and validated. Any failures and remedial action taken should be recorded.

17. A procedure should be established to record and analyze errors and to enable corrective action to be taken.

18. When outside agencies are used to provide a computer service, there

ANNEX 4: COMPUTERIZED SYSTEMS

should be a formal agreement including a clear statement of the responsibilities of that outside agency. (see chapter 8)

19. When the release of batches for sale or supply is carried out using a computerized system, the system should recognize that only an Authorized Person can release the batches and it should clearly identify and record the person releasing the batches.