GUIDELINES FOR DESIGNING USER INTERFACE SOFTWARE

ESD-TR-86-278

August 1986

Sidney L. Smith and Jane N. Mosier
The MITRE Corporation Bedford, Massachusetts, USA

Prepared for Deputy Commander for Development Plans and Support Systems, Electronic Systems Division, AFSC, United States Air Force, Hanscom Air Force Base, Massachusetts.

Approved for public release; distribution unlimited.

The body of this document is in the public domain
Table of contents and index © 1998 Userlab Inc.
www.userlab.com
1-800-295-6354
Contact us for additional copies
The only charge is for printing and shipping

DataDome Ex. 1012, p. 1
DataDome v. Arkose Labs
IPR2025-00693

THIS PUBLICATION IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

SUMMARY 5
ACKNOWLEDGMENT 5
INTRODUCTION 6
INFORMATION SYSTEMS 6
USER-SYSTEM INTERFACE 7
USER INTERFACE SOFTWARE 7
SIGNIFICANCE OF THE USER INTERFACE 8
DESIGN PRACTICE 9
DESIGN GUIDELINES 10
GUIDELINES ORGANIZATION 11
APPLYING THE GUIDELINES 13
ROLE OF GUIDELINES IN SYSTEM DEVELOPMENT 14
REFERENCES 15
GLOSSARY 33

1 DATA ENTRY 39

1.0 Data Entry: General 41
1.1 Position Designation 53
1.2 Direction Designation 59
1.3 Text 60
1.4 Data Forms 70
1.6 Graphics 84
1.7 Data Validation 100
1.8 Other Data Processing 101
1.9 Design Change 105

2 DATA DISPLAY 106

2.0 General 109
2.1 Text 118
2.2 Data Forms 128
2.3 Tables 134
2.4 Graphics 141
2.5 Format 175
2.6 Coding 180
2.7 Display Control 193
2.8 Design Change 210

3 SEQUENCE CONTROL 210

3.0 General 214
3.1 Dialogue Type 224
3.2 Transaction Selection 262

DataDome Ex. 1012, p. 3
DataDome v. Arkose Labs
IPR2025-00693

3.3 Interrupt 268
3.4 Context Definition 271
3.5 Error Management 274
3.6 Alarms 278
3.7 Design Change 279

4 USER GUIDANCE 279

4.0 General 283
4.1 Status Information 294
4.3 Error Feedback 301
4.4 Job Aids 308
4.5 User Records 318
4.6 Design Change 320

5 DATA TRANSMISSION 321

5.0 General 323
5.1 Preparing Messages 326
5.2 Addressing Messages 329
5.3 Initiating Transmission 334
5.4 Controlling Transmission 338
5.5 Receiving Messages 341
5.6 Design Change 346

6 DATA PROTECTION 346

6.0 General 351
6.1 User Identification 358
6.2 Data Access 361
6.3 Data Entry/Change 364
6.4 Data Transmission 370
6.5 Design Change 372

DataDome Ex. 1012, p. 4
DataDome v. Arkose Labs
IPR2025-00693

Comment: Some security experts recommend that passwords of nonsense material be composed by a computer and arbitrarily assigned to users, in order to make it more difficult for intruders to guess a password. Such measures will confound legitimate users more often than they will impede intruders, and are not recommended here. A better approach would be to keep passwords memorable, for initial system access, and then impose some auxiliary procedure to authenticate user identity in applications where passwords are considered insufficient protection.

Reference:

CSC-STD-002-85

Haskett 1984

6.1/4 Changing Passwords

Allow users to change their passwords whenever they choose.

Comment: A user may sometimes suspect that a password has been disclosed, and thus wish to change it.

Comment: In addition to optional changes by users, it may also be good security practice for a system to enforce password changes for all users at periodic intervals.

Reference:

CSC-STD-002-85

6.1/5 Private Entry of Passwords

When a password must be entered by a user, ensure that password entry can be private; password entries should not be displayed.

Comment: Covert entry of passwords will prevent casual eavesdropping by onlookers. This represents an exception to the general recommendation that all entries should be displayed.

Comment: In the interests of security, it might be noted that passwords should also not be retained in readable form in computer memory, although this is not an issue of user interface design.

Reference:

MS 5.15.2.2.3

CSC-STD-002-85

See also: 1.0/3

6.1/6 Limiting Unsuccessful LOG-ON Attempts

Impose a maximum limit on the number and rate of unsuccessful LOG-ON attempts that will provide a margin for user error while protecting the system from persistent attempts at illegitimate access.

DataDome Ex. 1012, p. 5
DataDome v. Arkose Labs
IPR2025-00693

Comment: Legitimate users will sometimes have difficulty completing a successful LOG-ON, perhaps due to inattention, or a faulty terminal, or faulty communications. Occasional LOG-ON failures of that kind should be tolerable to the system, with the user simply invited to try again.

Comment: A record of continuing failure by any particular user to complete successful LOG-ON procedures, including password entry and other tests of claimed user identity, may indicate persistent intrusion attempts. Repeated LOG-ON failures might thus be grounds for denying access to that user. Access might be denied temporarily for some computer-imposed time interval, or indefinitely pending review by a system administrator. The occasional inconvenience to a legitimate user may be tolerable in the interests of increased system security. Analysis of this tradeoff between convenience and security can determine the number and rate of LOG-ON failures that will be tolerated in any particular system application.

Reference:

CSC-STD-002-85

See also: 6.0/2

6.1/7 Auxiliary Tests to Authenticate User Identity

When system security requires more stringent user identification than is provided by password entry, devise auxiliary tests that can authenticate user identity without imposing impractical demands on users' memory.

Comment: Various means have been proposed for authenticating user identity, including the use of secret algorithms known only to each individual user. If computer-generated cues and user responses can be protected cryptographically from eavesdropping, a practical scheme might be to require a user to respond to a word association test individually devised by that user for this purpose.

Reference:

Haskett 1984

6.1/8 Continuous Recognition of User Identity

Once a user's identity has been authenticated, ensure that whatever data access/change privileges are authorized for that user will continue throughout a work session.

Exception: In special instances a user's data access/change privileges might reasonably change as a result of succeeding transactions, e.g., if computer analysis indicated suspicious or otherwise abnormal behavior.

Exception: A user might reasonably be required to repeat procedures for authentication of identity when resuming work after some specified period of inactivity.

DataDome Ex. 1012, p. 6
DataDome v. Arkose Labs
IPR2025-00693