"COMPANY COMPUTER USE POLICY"

Rules of Behavior w/Acknowledgement

Prepared for

COMPANY
123 Main Street
Washington, DC 20061

Prepared by:

L&N Technologies, L.L.C
www.ln-technologies.net

VERSION 1

DOCUMENT CHANGE HISTORY

Version	Date	Author	Description

TABLE OF CONTENTS

1.0 Introduction

Rules of Behavior are part of a comprehensive program to provide complete computer security. These guidelines are established to hold users accountable for their actions and responsible for I.T. security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program.

All users of "COMPANY" systems shall be trained on the Rules of Behavior for the systems to which they are granted access before receiving access. All users shall sign a statement acknowledging that they have received and understand the training.

Any failure to comply with the Rules of Behavior shall be considered a security incident. If the incident is deemed willful, it will be escalated to a security violation. Noncompliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

2.0 Responsibilities

"COMPANY" shall establish Rules of Behavior for each computer system and major application. The "BUSINESS OWNER" shall ensure that all users receive training concerning the Rules of Behavior and sign a statement acknowledging receipt of the Rules of Behavior.

Users are responsible for following computer system procedures to minimize security threats. Managers will conduct periodic reviews to ascertain that users are operating computer systems in a secure manner.

3.0 Other Policies and Procedures

The rules are not to be used in place of existing policy. They are intended to enhance and further define the specific rules each user must follow while accessing major applications.

User responsibilities shall be included in the computer system training "COMPANY" provides for users.

4.0 Work At Home

"COMPANY" may designate employees in specific categories (e.g., critical job roles, employees on maternity leave and employees with certain medical conditions) as eligible for working at home. Any work-at-home agreement should:

- Be in writing.
- Identify the time period the work at home will be allowed.

- Identify what "COMPANY" equipment and supplies will be needed by the employee at home, and how that equipment and supplies will be transferred and accounted for.
- Identify if telecommuting will be needed.
- Be reviewed by the manager prior to commencement.

4.1 Dial-in Access

No dial-in access will be used. All remote access to "COMPANY" must be done via SSL VPN access only and such access will only be granted by the "BUSINESS OWNER."

4.2 Connection to the Internet

Only authorized Internet connections will be allowed.

4.3 Protection of Copyright Licenses (Software)

"COMPANY" personnel shall comply with all copyright licenses associated with major applications, general computer systems, or commercial off-the-shelf (COTS) software. End users, supervisors, and functional managers are ultimately responsible for this compliance. LAN and PC users shall not download LAN-resident software. Audit logs will be reviewed to determine whether employees attempt to access LAN servers to which users have not been granted access. Unauthorized copying of PC-based software is also prohibited.

4.4 Unofficial Use of Government Equipment

Users should be aware that personal use of "COMPANY" information resources, applications, networks, LANS, and PCs is normally not authorized. However, under certain conditions, limited personal use of "COMPANY" office equipment, including information technology resources, is authorized.

4.5 Use of Passwords

Users shall follow "COMPANY" password management rules. Users shall keep passwords confidential and not share passwords with anyone.

4.6 System Privileges

Users are given access to major applications or computer systems based on a need to perform specific work. Users shall work within the confines of the access allowed and shall not to attempt access to systems or applications to which access has not been authorized.

4.7 Individual Accountability

Users will be held accountable for their actions on all "COMPANY" applications and systems. This accountability shall be stressed during computer system awareness training sessions.

4.8 Restoration of Service

The availability of "COMPANY" systems and applications is a concern to all users. All users are responsible for help facilitating the restoration of services in the event a major application or computer system is not operational.

4.9 Acknowledgement

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for "COMPANY" major applications and computer support systems.

_____ _____

Signature of User Date