CLEAN DESK POLICY

1. OVERVIEW

ConectUS Wireless is committed to developing security policies and practices and, in doing so, has implemented this clean office policy to increase physical security in ConectUS Wireless's offices.

A clean office policy is a powerful tool to ensure that all sensitive/confidential documents are removed from the end user's workspace and locked when items are not used or when an employee leaves the workstation. The goal is to minimize the risk of security breaches in the workplace.

2. PURPOSE

The purpose of this policy is to ensure that confidential information and sensitive documents are kept away from inquisitive eyes when they are not used by authorized personnel or when the employee leaves his or her workspace.

This policy is also intended to increase employee awareness of the protection of sensitive information.

3. OBJECTIVE

The objective of this policy is to establish minimum requirements for maintaining a "clean office", where sensitive/critical information about employees, intellectual property, customers, partners and suppliers is protected in locked areas and out off site.

A Clean Desk policy not only complies with the highest industry protection standard but is also part of the standard basic controls for confidentiality.

4. SCOPE

This policy applies to all current employees and affiliates of ConectUS Wireless, including full-time and part-time, contractual, permanent and temporary employees and also applies to job applicants.

5. POLICY

a) Employees are required to protect all sensitive or confidential information in their workspace at the end of the working day and when they are absent from their workspace for a prolonged period of time. This includes electronic and physical hardcopy information.

b) Whiteboards containing confidential and/or sensitive information should be erased after use.

c) If you are not sure that a duplicate of a sensitive document should be kept, it is probably better to place it in the locked shredder bin.

d) Consider scanning paper items and filing them electronically in your workstation.

e) Desktops/laptops must be locked (disconnected or turned off) when left unattended and at the end of the working day. Portable devices such as laptops and tablets that stay overnight in the office should be turned off and stored out of sight.

f) Laptops must be either locked with a locking cable or locked away in a drawer.

g) Keys used to access restricted or sensitive information and physical access cards should not be left unattended on a desk.

h) Any restricted or sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.

i) Mass storage devices such as CDs, DVDs, USB drives or external hard drives must be treated as sensitive material and must therefore be in locked locations when not in use.

j) File cabinets containing restricted or sensitive information must be kept closed and locked when not in use or when not attended.

k) Printed documents should be immediately removed from printers or fax machines. Printing of physical copies should be limited and reserved only for documents requiring a physical copy. Documents should be accessed, shared and managed electronically in most cases.

l) At the end of the day, any documents remaining in the printer must be put in the shredding bin.

m) The documents remaining in the fax must be put in a folder intended for this purpose and this folder must be put in a binder and locked at the end of the day.

n) All sensitive documents and restricted information that must be destroyed, must be placed in locked confidential shredding bins.

o) Passwords should not be left on sticky notes displayed on or under a computer or written in a place that is accessible to everyone.

6. ENFORCEMENT

Employees are expected to follow the spirit and intent of this policy. Periodic sweeps of work areas may be conducted by their supervisor or his designee during non-work hours to verify adherence to the policy. Violations will be brought to the attention of the respective supervisors for appropriate follow-up action.

7. MANAGER RESPONSIBILITY

It is the responsibility of any department manager to ensure that the above policies are implemented.

Repeated or serious violations of the office's Clean desk policy may result in severe disciplinary action up to and including dismissal.

8. MISSING DOCUMENTS OR DEVICES

If you notice that any of your devices or documents have disappeared, or if you think your workspace has been searched or manipulated in any way, please inform **JoAnne Scully** right away.

9. EMPLOYEE AGREEMENT ON CLEAN DESK POLICY

I acknowledge that I have received a copy of the **ConectUS Wireless** clean desk policy. I have read and understand the policy. I understand that, if I violate the policy, I may be subject to disciplinary action, including termination. I further understand that I will contact my supervisor if I have any questions about any aspect of the policy.

Dated: _____

EMPLOYEE	CONECTUS WIRELESS
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Print Name and Title	Print Name and Title