



People First; Mission Always

Corporate Capabilities for Government Customers

ManCom Inc.

ORGANIZATIONAL INFORMATION

SPECIFIC MANCOM INFORMATION	
Organization Name	Management Communications Inc. (ManCom Inc.) S-Corporation
Address	8601 N. Black Canyon Hwy, Ste 117 Phoenix, AZ 85021
POC Contact / Email Address	Yolanda Hernández Cruz Chief Financial Officer yhernandez@mancominc.com
Business Type	Small Business
Telephone / Fax	(623)236-3500 / (623) 217-2413
Designations	8a: VOSB SBE DBE GSA-70, HUBZone
TIN	45-4921076
DUNS #	078579107
CAGE Code	6Z0K7
NAICS Codes	541330 541511 541512 541513 541519 541611 541618 541690 561110 561210
GSA Schedule 70	47QTC A19D00LD
Military Critical Data Handling Cert.	Certification # 0068922 (DD2345)
Website	www.mancominc.com



Contact Us At 623-236-3500
We are available **24x7x365!**

Corporate Capabilities for Government Overview

Executive Summary

Management Communications Incorporated (ManCom Inc.) is a certified Veteran Owned Small business that has been in business since 2012. Our Management and Executive Team has more than 60 years of combined experience supporting federal, DoD, state, local US Government agencies as well as schools, universities, and libraries.

ManCom is a Microsoft certified Cloud Solutions Provider (CSP) that brings years of experience supporting and providing training for **Microsoft SharePoint**, Teams, One Drive and other 365 and cloud services. We are an authorized Microsoft 365 license advisor with a thorough understanding of the Microsoft 365 Academic Licensing use case, cost discounts and purchasing strategies.

We are one of the few small businesses that provide Microsoft licensing, consulting and application development services which makes us uniquely and expertly qualified to support the College of Charleston. ManCom currently provides Microsoft 365 and SharePoint training, development, migration, updates from "Classic" to "Modern View", consolidation with Teams and One Drive. Our team has developed sites for small, medium, large, and very large organizations to support records and document management, document retention, Section 508 Accessibility, data governance and other task objectives related to Microsoft 365 Cloud Applications.

ManCom is located at 8601 N. Black Canyon Highway, Suite 117 in Phoenix Arizona. Within our facility is our Executive and Management Team, technical and administrative staff, shipping and receiving, finance and accounting as well as our subject matter experts for technical support, licensing, website development, records management, and digitalization services. Additionally, our facility contains a lab that is used for test and evaluation, media conversion and other task requirements currently provided to support federal, state, academic and commercial customers.

Darrell Leonard

President | Chief Executive Officer



A Veteran Owned, 8(a), Hub Zone Small Business

DUNS Number 078579107

NAICS CODES: 541511 541618 541512 541690 541513
561110 541519 81121 238210 811213 541611 811219

CAGE CODE # 6Z0K7 JCT # 0068922

SBA 8(a) VOSB SBE/DBE # 20190665

SPIN # 143036825

CAPABILITIES STATEMENT



Management Communications Incorporated (ManCom Inc.) is a Veteran Owned, 8(a), Minority Small Business, certified by the State of Arizona as a Disadvantaged Business enterprise (DBE) and the City of Phoenix as a Small Business Enterprise (SBE).

ManCom delivers a broad range of information technology, management and technical services solutions to Commercial, U.S. Federal, State, Municipal Government and Commercial customers focusing primarily on critical Information Technology Engineering, Cyber Security, Network Architecture Design, Systems Integration, Systems Administration, Strategic Planning, Staff Augmentation and Program Management.

We provide specialized support, with round-the-clock availability, in the following areas: Program Management, Logistics, Installation telecommunications systems/network, VoIP and POTS Support Services, Unified Communications, Operations and Maintenance (O&M), Website development and Digital Marketing, SEO, Microsoft 365 integration and migration, SharePoint, ISP Management, ROI Analysis, System Lifecycle Support, Equipment and Software Procurement, Strategic Planning, Manpower, Training, Testing and Evaluation, Technical Documentation and Engineering, Design services.

Technical Service Offerings

- Network Assessment
- On/Off-site data storage
- Security audits
- Voice/Data Operation and Maintenance
- Strategic Planning
- On-demand services
- CMMI Business Continuity Planning
- ISO Business Management Planning
- Wireless Network Engineering
- Adds/Moves/Changes

- HIPPA Preparation and Documentation
- HIPAA Compliance Surveys
- On-site Service
- Remote monitoring
- Managed Services
- Network Engineering & Services
- VOIP and POTS Phone Systems
- Surveillance Camera Systems
- Unified Communications
- Remote help desk

- IT Staff Augmentation
- Low Voltage Cabling
- Alert reporting
- Internet and phone line audits
- Card /Biometrics Access
- On-going service agreements
- Network Engineering and support
- Product procurement
- ROI Analysis Lifecycle Support
- Website Development & SEO
- Content & Social Media Management

People First; Mission Always

MANCOM SILO'S				
IT CONSTRUCTION REBUILD	IT SERVICES	MICROSOFT CSP LICENSING	TRAINING	SHAREPOINT
<ul style="list-style-type: none"> - New equipment and cabling - Design and Consultation 	<ul style="list-style-type: none"> - Full IT Services - Cyber Audits - Consulting - Procurement 	<ul style="list-style-type: none"> - Certified Microsoft - Discounted Licenses - Government Licensing with Azure 	<ul style="list-style-type: none"> - Certification Training 	<ul style="list-style-type: none"> - Website Design - Administration

8601 N. Black Canyon Hwy, Suite 117 Phoenix AZ 85021 | Phone 623.236.3500 | Fax: 623.217.2413 | mancominc.com

Why Us?

For US government agencies, ManCom provides cloud services that must meet government security and compliance requirements.

- ✚ Microsoft AZURE for government – physically isolated datacenters and networks (located in U.S. only) to provide highest level of security & compliance services.
 - FedRAMP
 - NIST 800.71
 - ITAR
 - IRS 1075
 - DoD L4
 - CJIS



ManCom validates each cloud computing element as a quality standard and integrates it into each separate cloud computing service offering. ManCom cloud computing services have inherent controls focused on NIST 800-145 to support DFARS compliance. ManCom recommends solutions that provide shared resources in a secure environment while aiding in the drafting of policies that substantiates business processes and data retention in a cloud environment. ManCom focuses on all levels of controls to include Access Control, Awareness, Accountability, Configuration Management, Identification and Authentication, Physical Protection, Risk Assessments, System and Data Integrity, Incident Response, Maintenance and Training. Other levels of controls are supported in our quality surveys and action planning.



With a dedicated focus, ManCom ensures your infrastructure & telecommunications needs are managed & maintained with regard to the end user & mission objectives. Our focus is built on principles of Ethics, Morality, Honesty, and Integrity. "People First – Mission Always!" Small Veteran Owned Minority HUBZone Business with over 60+ years combined experience in all facets of IT Support Management, Operations, Finance & Accounting, Network Engineering, Cyber Security and Strategic Planning.

Joanna Sweatt | 623.236.3500 ext. 493

jsweatt@ManComInc.com

8601 N Black Canyon Hwy, Suite 117, Phoenix AZ, 85021

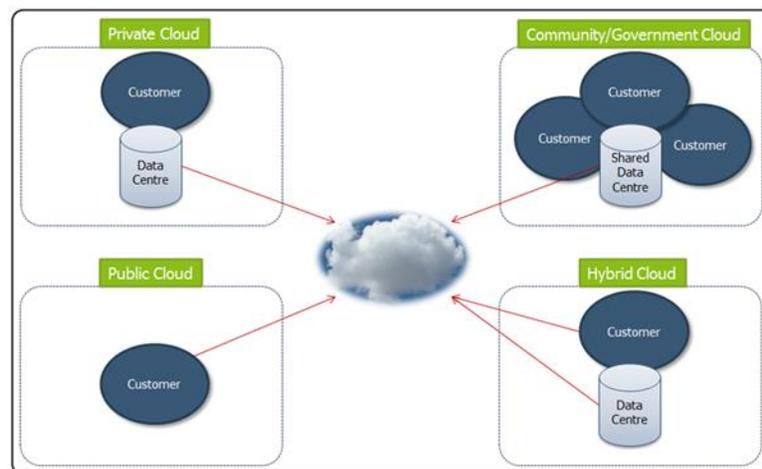
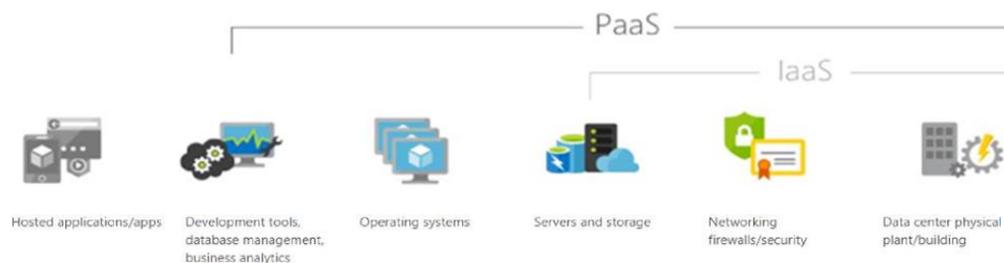
Secure Cloud Services & Capabilities

All shared resources in a common environment are safeguarded at high or moderate levels depending on the customer or tenant. ManCom understands the evolution of technology in the cloud computing environment and is aggressively working with original equipment manufacturers to ensure they understand the nuances of NIST 800-145.

For US government agencies, ManCom and any subcontracting partner providing cloud services must meet government security and compliance requirements. An example of supporting network access is Microsoft Azure for Government. Azure Government provides world-class security, protection and compliance services that are utilized as broad network access. Azure Government delivers a dedicated cloud enabling government agencies to transform mission-critical workloads to the cloud. Azure Government services handle data that is subject to certain government regulations and requirements, such as FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L4, and CJIS. Azure Government uses physically isolated datacenters and networks (located in U.S. only) to provide the highest level of security and compliance services.

Azure Government customers include only those agencies that are US federal, state, and local government or contractors that support government requirements. Typically, we strongly recommend all contractors supporting US Government requirement maintain Azure Government and Office 365 GCC Tenants to ensure compliance.

ManCom provides NIST compliant software applications that has been vetted and approved as recommended solutions to our customer base. Applications such as, but not limited to Azure, data and network support center operations, Microsoft 365 GCC are just a few that provide and ensure compliance with NIST Standards. Our proposed services require all personnel to include all OEM's that provide services in support of our customers are U.S. Citizens, all data is protected by individual and approved firewalls. Data is encrypted and housed within the continental United States. Our services are constantly monitored and measured against our Quality Control Plan and Surveillance Plan (QASP) and vetted against our Quality Plan.



*Bonus Capability

ManCom is an industry advisor for the Federal Government concerning modernization, electronic document management systems and the overall improvement of the government's digital strategy.

-ManCom's President & CEO is on a Digital Governance Senior Steering Committee and various Cross Functional teams

-ManCom's solutions are secure, out-of-the-box, customizable, and within compliances with all Federal Regulations

Security is always the PRIORITY in Digital Strategies and ManCom is committed to protecting and transforming the government's IT culture

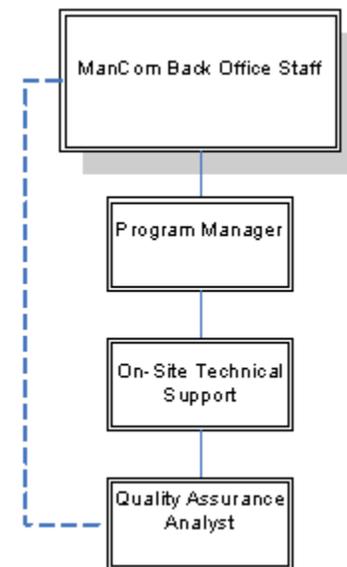
ManCom's Commitment to Cyber Security

ManCom takes Cyber Security very seriously; therefore, we place the highest level of attention to your network infrastructure and ensuring that you are protected from threats as our first integration metric working with your agency or business.

At ManCom, we view **cyber security** from a granular level with an understanding that **Cyber Security** is not only hackers attempting to break past your firewall and wishing to breach or disrupt your business practice but, '**Cyber Security**' is much, much more.

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and **cyber security** describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of **cyber-attacks grow**, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation's top intelligence officials cautioned that **cyber-attacks and digital spying are the top threat to national security**, eclipsing even terrorism (De Groot, 10/5/2020 *Digital Guardian*).

We plan to leverage as much information gathered and provide solutions to our customers to ensure they are aware of **cyber threats** that may exist within their network architecture and how to mitigate them. Prior to, during, and after the migration, we will review and test policies and procedures with data security and **cyber policies** as critical factors in all areas. Our extremely knowledgeable **cyber security team** will ensure all internal policies as well as Einstein3, the 2018 FISMA Metrics, OMB M17-25, and the DHS NIST **Cyber Security Framework** are measured, corroborated, implemented, and maintained. Our team is expertly qualified in implementing and supporting **Federal Cyber Security Mandates** and will provide detailed reporting on security status throughout the process. Additionally, we will provide recommendations with details on how recommended solutions will increase current security standards and apply to policies and mandates.



Top Identified Cybercrimes

1. Phishing Scams
2. Identity Theft Scams
3. Online Harassment
4. Cyberstalking
5. Invasion of Privacy

ManCom stays abreast of cybersecurity news in our rapidly evolving world of cyber threats. ManCom is engaged with the most relevant cybersecurity vulnerabilities, advisories, and news for our U.S. Federal government customers.

Cyber Security Capabilities

ManCom knows that Cyber Security starts with understanding your business's mission and capabilities and assessing potential threats by evaluating your current infrastructure and determining the appropriate course of action(s) in the discovery phase to include ensuring the authenticity of the products you are utilizing. In addition, ManCom collaborates via joint ventures and teaming agreements with some of the industries top Cyber Security SMEs.

Phase I Discovery

Facilities and Physical Controls

- On site review of facilities, document controls and access
- Discussions with leadership operations and staff
- Findings and Recommendations Report

Email Accounts, Users and Logical Controls

- Email Encryption – Zix Email Encryption
 - Email Threat Protection
 - Email Encryption
 - Secure File Share
- Verification process with Microsoft and your Agency/Organization
- Convert standard accounts to Government Email accounts

Phase II Developing a Compliance Plan

Compliance Plan

- Plan to include changes required to comply with 252.204.7012 / NIST 800-171
- Plan addresses and provides an outline applicable to all phases of compliance
- Hardware or other cloud services - Creating a secure documents repository and relocating files and archived documents (SharePoint)
- Site Content Maintenance and Permissions
 - Incident Response Plan

