INTEGRATED COMPUTER SYSTEMS

شركة المترابط لأنظمة الحاسب الآلي

Integrated Computer Systems

75, Zuhair Bin Abi Salma St., Al Maseef Dist.,
Riyadh, Kingdom Of Saudi Arabia
P.O.Box. 28612 Riyadh 11447

+966 11 494 3010
+966 11 494 3020
info@ics.sa

OVERVIEW

ICS is a Saudi company was formed over 15 years ago to provide integrated solutions to the Saudi market. We are a fast-growing provider of information technology services and multidisciplinary business solutions in the Kingdom.

ICS integrates its wide range of capabilities to help companies appreciate the benefits of information technology once employed. ICS has the necessary skills to provide a comprehensive assessment of how an organization fits within the information technology environment.

Since its foundation, ICS has evolved from being a regional system integration establishment, to an internationally acclaimed integrated solutions company. We work with a network of national and international allies to provide cutting-edge technologies in ICT solutions, services and support. Those are designed to maximize our clients' investments and meet their objectives with minimal cost; benefiting from existing ICT infrastructure.

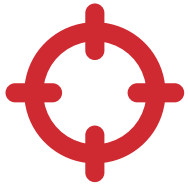
OUR WORK INCLUDES:

- Security
- Telecommunication
- Datacenter Critical Facility
- Sftructured Cables
- Converged Network Infrastructure

VISION, MISSION AND VALUES

VISION STATEMENT

Our vision is to be a world class company, a company renowned as a competent leader in the ICT arena setting the benchmark for all others, providing solutions from vendors that are globally recognized.



MISSION STATEMENT

Our mission is to be innovative in delivering Information and Communication Technology (ICT) solutions and services that support our clients in achieving their business objectives deploying industry world leading best practices. We are committed to invest in technology and people ensuring sustained growth, building excellent career paths and evolving local Saudi national expertise.

VALUES

Colleagues, Clients, and Company; are the core values of ICS. Understanding the needs of these values stands at the essence of our company, and enables us to fulfill our mission to be innovative, customer-focused and a great workplace.

STRATEGY

BUSINESS GOALS & OBJECTIVES

Deliver Information and Communication Technology (ICT) solutions and services to the Saudi Market. By leveraging our expertise, we work closely with our customers to comprehend and fulfill their needs and exceeding their expectations.

Use advanced and modern approaches in employing and developing our staff, creating teams or experts that are capable of undertaking the most challenging and demanding projects.

Continuously review, improve, and develop our processes creating innovations and tailoring our company to be the most flexible, the best fit and the most novel.

Our objective is to deliver solutions that deliver real value to our customers.

WHERE ARE WE HEADED?

Our past, growth and the proven track record in the last 16 years, demonstrate our exceptional achievements. Thus, we can confidently forecast a bright, full of challenges and successful future for ICS. We will keep on planning, we will stay focused and work hard to accomplish our mission, in the view of our vision and the appreciation of our values.

SERVICES >

SECURITY SOLUTIONS & SERVICES

Our range of internationally accredited security solutions and services covers the whole spectrum of security technology. This includes Cyber Security solutions, holistic IT conceptions and security services, in addition to telecommunications, surveillance and access control systems.

FOR THIS WE OFFER VARIOUS SECURITY SERVICES SUCH AS:

- Link Encryption
- Email Security
- Professional Firewalls
- File and Email Encryption
- Cyber Security
- Intrusion Prevention Systems (IDP)
- Digital Forensics
- Data Leakage Prevention (DLP)
- PKI and Digital Signature Solutions
- Surveillance Parameter Security

INTRODUCTION

Security is becoming more and more established in the corporate structure, it is no longer acceptable for security to be a secondary function of an IT department. To address this challenge, organizations are investing in the development of security operations centers (SOCs) to provide increased security and rapid response to events throughout their networks.

Building a SOC can be a massive task. Although the finer points of SOC deployment are very much network-specific, there are several major components that every organization must include: **people, process, and technology.** The three exist in all elements of security and should be considered equally critical Components. Our approach explains how strong people, well-defined processes and state of the Art technology can result in an operationally effective SOC.

Our approach is a holistic one that combines both Defense-in-Depth & Adaptive Security mindsets that builds flexible, deeply integrated framework that offers a far-reaching view of threats and evolves as quickly as conditions do. Rather than only trying to prevent every attack, implementing an adaptive model recognizing that some attacks will get through. Changing mindset and aim to quickly detect attacks and then respond forcefully to prevent the worst results if an attack got through.

An end to end solution that starts with defining the Security Posture of your organization; defining to what extent are you practicing Confidentiality, Integrity & Availability of your information, how effective you are in addressing cyber- attacks and ending with well-defined Incident Response capabilities that will support forensics investigations, with SOC at the heart of it.

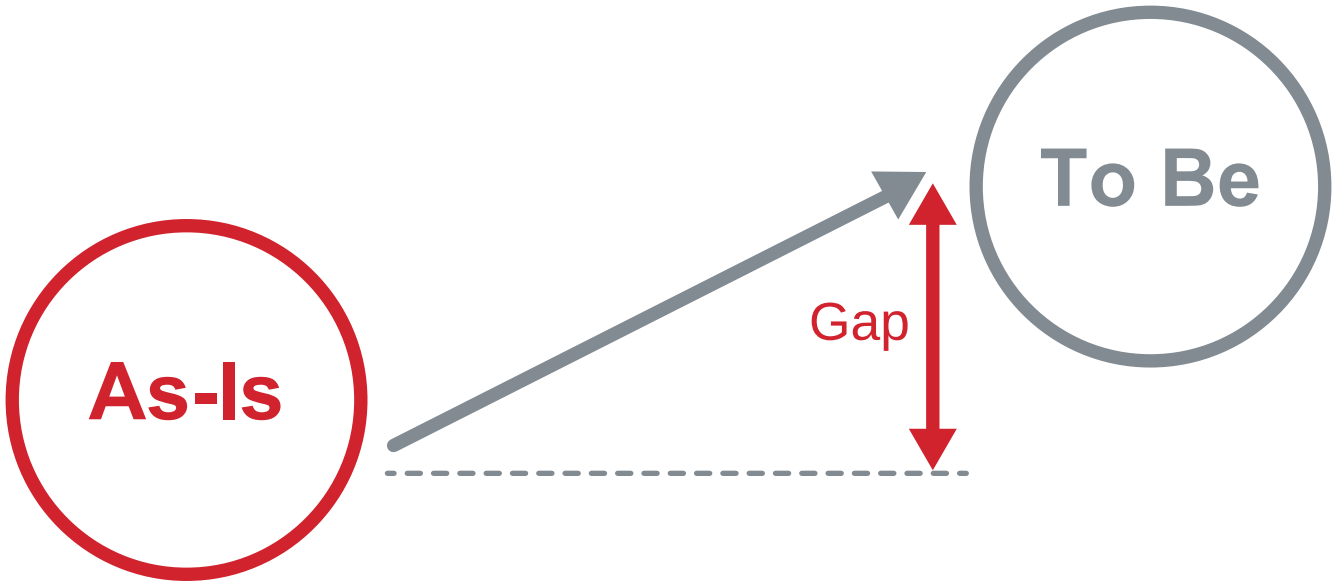
DEFINE SECURITY POSTURE

The primary objective of this phase is to understand the current security posture of the organization (As-Is) and based on the fining define the desired security posture to achieve upon addressing the recommendation and putting the required controls in place (to-Be). This start with conducting As-Is cyber security vulnerability assessment to all public and private infrastructure and campus connectivity infrastructure. The As-Is assessment usually covers the following areas:

- **Review IT and network systems, topologies, and external boundaries for cyber vulnerabilities**
- **Review information technology related policies from security standpoint**
- **Identify critical cyber targets including commercial infrastructure that may affect business operations**

The expected outcome of the As-Is phase is an information security risk assessment report highlighting the security posture and risk status of the cyber protection systems based on ISO27k controls and highlighting the recommended action to mitigate risks.

Develop a To-Be high level security architecture taking into consideration the findings from the As-Is phase and the international best practices. Develop implementation roadmap to help you prioritize the desired cyber security initiatives.



BUILDING A SOC

SOC COMPONENTS

- **Define the security operations center**
  (Mission, Scope & Responsibility)
- **Determine the processes**
  (Templates & Procedure)
- **Understand the environment**
  (Scope of work and domain to be monitored)
- **Staff the SOC**
  (Staff, training & Operational Hours)
- **Manage the events**
  (Prioritize, correlate and manage events received)
- **Facilities to host the SOC**
  (Facility, Layout)

DEFINE THE SECURITY OPERATIONS CENTER

The first and most important component when implementing a SOC is to define the mission, charter, objectives, and responsibilities.

- **Mission**
- **Charter**
- **Objectives**
- **Responsibilities**
- **Operational Hours**

Once the responsibility definition has been documented, a list of service functions for the SOC must be defined. The service functions, once defined, will guide the daily processes and procedures for the SOC staff. Once each service is defined, each resource within the SOC can be assigned a series of responsibilities based on each individual's expertise.

Once each service function is defined, a series of documents must be developed to ensure the appropriate information is gathered during an event or incident and to ensure consistency across all SOC staff.

DETERMINE THE PROCESSES & TEMPLATES

The number of processes and procedures for a SOC is determined by its scope, how many services are offered, the number of customers supported, and the number of different technologies in use. An established SOC environment may have tens or even hundreds of procedures. At a minimum, the basic procedures that are required for maintaining the SOC are:

- **Monitoring procedure.**
- **Notification procedure**
  (email, mobile, home, chat, etc.).
- **Notification and escalation processes.**
- **Transition of daily SOC services.**
- **Shift logging procedures.**
- **Incident logging procedures.**
- **Compliance monitoring procedure.**
- **Report development procedure.**
- **Dashboard creation procedure.**
- **Incident investigation procedures**
  (malware, etc.).

Many of the procedures listed above may need to be customized based on the type of technology in use.

REQUIRED TEMPLATES

A series of baseline templates should be created to help maintain documentation consistency by establishing the same format and basic information sets across policy and procedure documents.

For example, templates for proper data input into ticketing systems and the GRC system will need to be developed to help ensure the appropriate technical information is gathered. A few key templates required are:

- **Shift log templates for each use case.**
- **Templates for each incident trouble ticket category.**

REPORTING PROCESS

As a primary function, regular reports will need to be generated and provided to different audiences within the organization. Usually a weekly report is prepared for incidents, detailing the activity within the SOC. These reports can be delivered to management and other members on the core escalation contact list.

Proper reports should be in place for the SOC team to:

- **Review all incident records regularly to ensure they were resolved within the parameters of the defined severity levels.**
- **Audit incident records that have exceeded standard resolution times to validate that the incident records were handled appropriately.**
- **The SOC processes and procedures should be reviewed regularly and updated based on the report data reviews and audits.**
- **In addition, many other reports can be created depending on the type of data received or requested by management.**

UNDERSTAND THE ENVIRONMENT

Without an understanding of the technical environment, it will be difficult to investigate and to understand if an actual attack has occurred. For this reason, the staff within the SOC must have the appropriate tools, diagrams, and knowledge of the network to perform their daily job. It is important to have both an electronic and a hard copy of the key network and application architecture diagrams.

For any new SOC staff, navigating and understanding the environment should be included as part of their required basic training. This will also help meet SLAs and overall customer service within the SOC.

As a part of the SOC's service functions the security architecture will be defined and the SOC staff will have access to the different components and tools within that architecture. These may include, but are not limited to:

- **SIEM monitoring and correlation.**
- **Antivirus monitoring and logging.**
- **Network and host IDS/IPS monitoring and logging.**
- **Network and host DLP monitoring and logging.**
- **Centralized logging platforms** (syslog, etc.).
- **Email and spam gateway and filtering.**
- **Web gateway and filtering.**
- **Threat monitoring and intelligence.**
- **Firewall monitoring and management.**
- **Application whitelisting or file integrity monitoring.**
- **Vulnerability assessment and monitoring.**

ACTIONABLE EVENTS

To ensure the SOC is effective, a series of actionable events list must be defined. Think of these as **events that require SOC intervention and/or monitoring.** For instance, a repeat attack from a single source is an actionable event. It's an actionable component of the SIEM in which the SOC was notified of, through the network's primary monitoring tool. These may include the involvement of a **Rule, Alarm, or even a Dashboard** to meet the organization's requirements. Before defining them, it is important to have a firm grasp on the company policy, its assets, and the technical environment. A good way to develop Actionable Events is by viewing the network from an attacker's perspective; think of a disruption to the environment. Another option is to look at the regulations the organization is subject to and evaluate the items that could become non-compliant. The development of this list is a critical component within a SOC and it must be understood.

STAFFING THE SOC

Staffing a SOC can be more difficult than expected. Two questions that executives ask are:

- **How many employees do I need?**
- **What skill sets are required?**

The number of employees is dependent on the operating hours of the SOC. If the operations are maintained 24 hours a day, seven days a week, not only do shifts need to be considered, but you will also need to consider time off, sick days, and holidays. A standard 24-hour SOC must be maintained by at least seven staff members. If not, procedures should be put in place for off-hours monitoring. This enables the staff to have a one-hour overlap for shift transfer and a floater to cover any holidays or time off when needed.

Finding the right skills and hiring staff is a difficult task at the current time because there are a limited number of security professionals in the market. The security staff within the SOC must have a solid background in many different aspects of computer technology usually focusing on networks, applications, and in some cases, reverse engineering. In addition, a good manager or director is required to ensure documentation, optimization, and reporting are maintained appropriately. Typical roles within a SOC may include:

- **Security Analyst.**
- **Security Specialists.**
- **Forensics or Threat Investigators.**
- **Manager or Director.**

EVENT MANAGEMENT

The core function and technology within a SOC are based on events from hundreds or even thousands of different systems. Essentially the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon. The management of events must include a list of instructions that apply on a 24x7 basis. This does not necessarily have to be the Incident Response Program Guide or Handbook. An event is any element that comes into the SOC and is monitored; while an incident is an event that must be acted upon.

As a part of event management, the SOC provides telephone and email assistance to its customers covering some of the following areas:

- **Malware outbreak.**
- **Phishing attacks.**
- **Social engineering calls.**
- **Access to the organization's security portal.**
- **Data leak/loss incidents.**
- **Customer account lockout.**
- **Customer inquiries.**

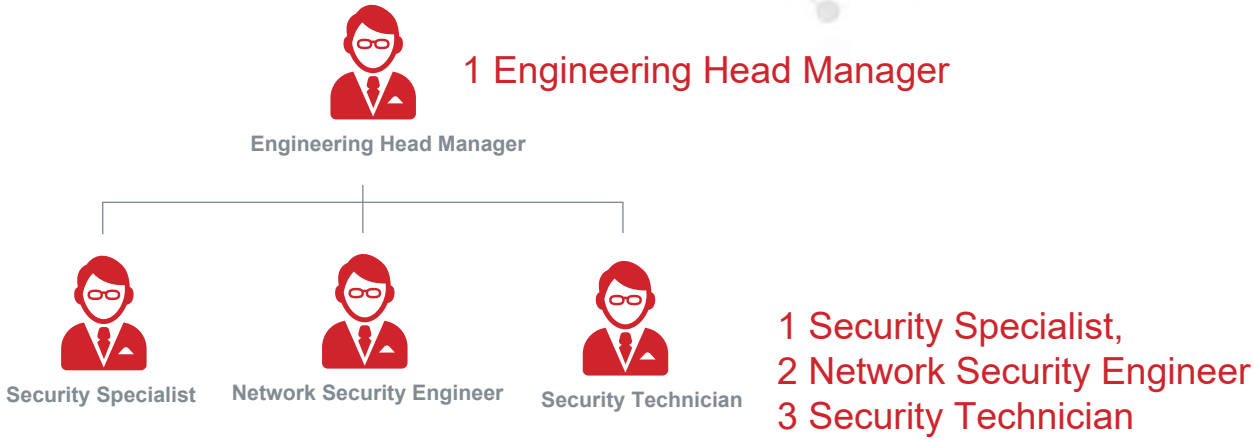
SERVICES >

Security Random References

Project Name	End User
Email Gateway Security	Confidential
Gaurd 3 (Next Generation Firewall)	Confidential
Gaurd 3 (Identity Service Engine)	Confidential
Advanced Persistent Thread	Confidential

SERVICES >

Security Teams

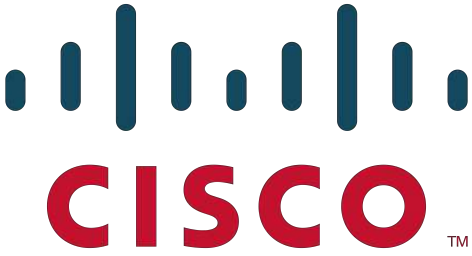


1 Engineering Head Manager

1 Security Specialist,
2 Network Security Engineer
3 Security Technician

SERVICES >

Security Partners



SERVICES >

Structrued Cable Services (ISP/OSP)

DESIGN AND PLAN

- Site Survey Conducting
- Route identification
- Layout Digram Design
- Bill of Quantity (BoQ) Building

DEPLOYMENT

- Horizontal and Core Cable Pulling
- Fiber Splicing and termination
- Trenching and Civil Work
- Cabinet Installation and Organization

Testing

- Fiber Testing and Comssioning
- UTP Testing and Comissioning

DOCUMENTATION AND MAINTENANCE

- Test Result Documentation
- As Built Documentation
- Ticketing System for Cable Maintenance









SERVICES >

ISP/OSP Equipment

Equipment Name	Quantity
Loader JCB	3
Trencher	2
Bob Cat	2
Air Compressor	4
Dyna Truck	3
Wheel Meter	3
Cable Locater	2
Cars, pickup	20
HILTI	3
Asphalt Cutter	3
Splice Machine	5
OTDR	5
Power Meter	10

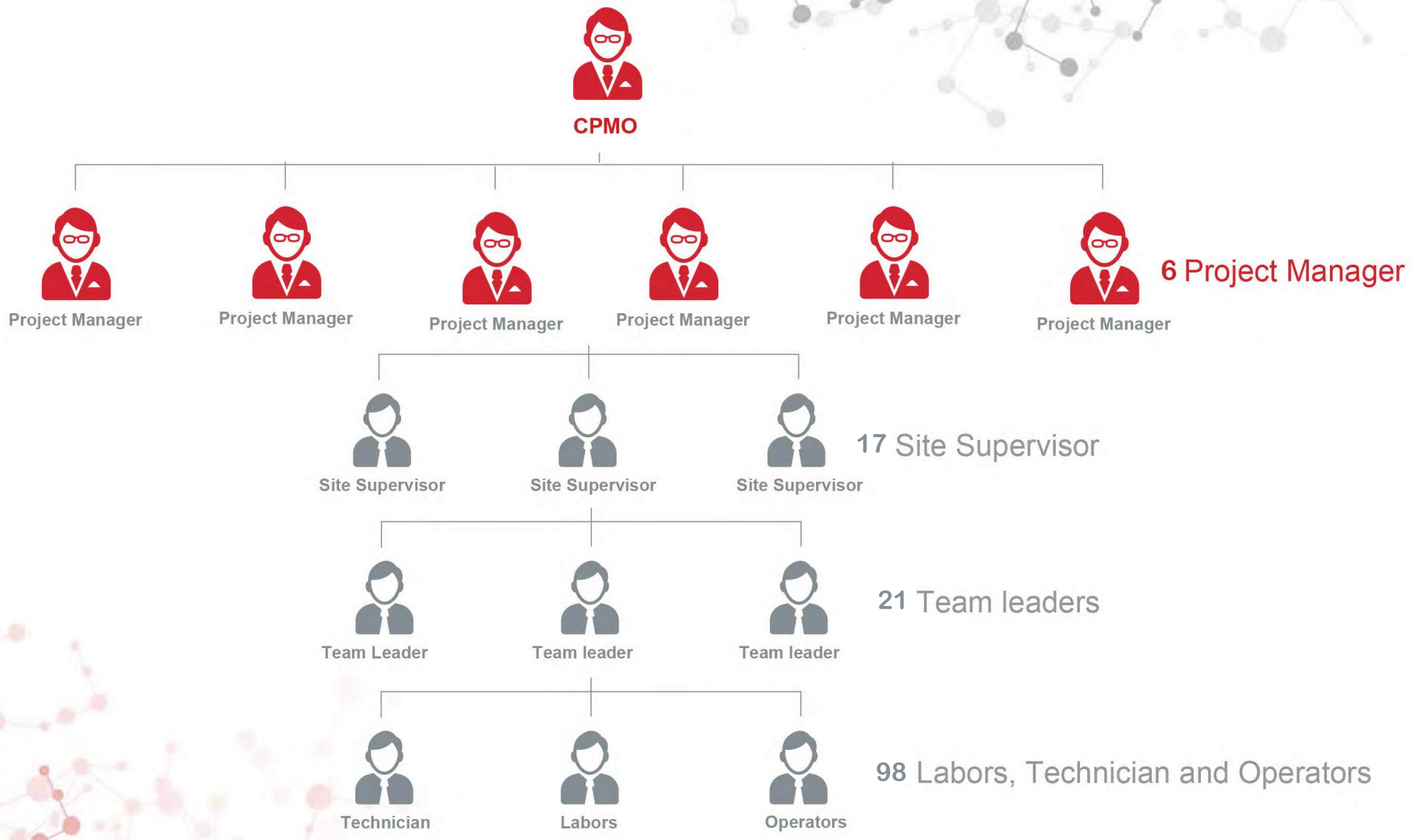
SERVICES >

ISP/OSP References

Project Name	UTP Nodes	Fiber	Customer/End user
Network Expansion Phase 2	3500	160 km	Royal Saudi Air Force - RSAF
DSL Infrastructure Project	6319	261 km	Baud Telecom Company
Emdad Infrastructure Phase 1	0	250km	Advance Electronics Company Limited
Emdad Infrastructure Phase 2	0	274km	Advance Electronics Company Limited
Emdad DDCE Infrastructure	4418	204km	Advance Electronics Company Limited
IP Telephony phase 1	4500	220km	Saudi Buisness Machines
IP Telephony phase 2	4000	120km	Saudi Buisness Machines
Radar HSN Connectivity expansion	3500	160km	Northrop Grumman Corporation
Wireless Infrastructure	1132	7.5km	University of Hail
Wireless Infrastructure	270	7.1km	General Authority of Civil Aviation
Fiber Infrastructure Project	5500	158km	Royal Saudi Naval Force
ACS MODA Network Enhancement	2000	0	Arabic Computer Systems
MOC Network Enhancement	2000	1.6km	Ministry of Culture & Information
SMF Network Enhancement	1150	0	Strategic Missile Force
F 15 Fleet Modernization Program	1069	5 km	CDMSmith

SERVICES >

ISP/OSP Teams



SERVICES >

ISP/OSP Clients

STC الاتصالات السعودية ADVANCED SOLUTIONS

AEC

BTC Networks

SBM SAUDI BUSINESS MACHINES

Honeywell

NORTHROP GRUMMAN

القوات الجوية الملكية السعودية

القوات البحرية الملكية السعودية

GACA الهيئة العامة للطيران المدني General Authority of Civil Aviation

جامعة حائل University of Ha'il

SERVICES >

ISP/OSP Partners

SERVICES >

Telecomm-unication

Point to Point and Point to Multi point Radio:

- Base Transmission Station Installation and Configuration
- Shelter Installation
- Network Integration

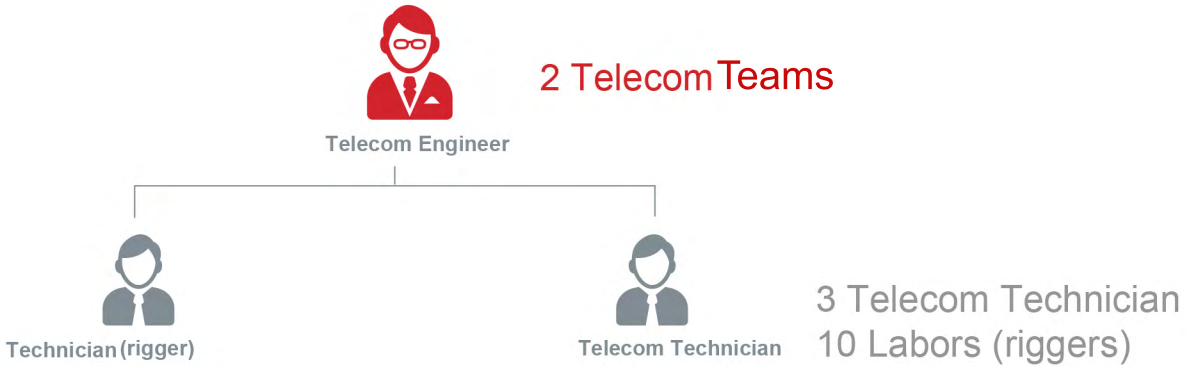
Tower Work

- Antenna and cable type identification
- Antenna Installation
- Cable Pulling
- VSWR Cable loss
- DTF Test

Telecom References

Project Name	End Unser
DTRS Project Phase 1	Royal Saudi Air Force
DTRS Project Phase 2	Royal Saudi Air Force
Comm. Equipment Upgrade Project	King Faisal Air Academy
Comm Equipment Project	King Faisal Air Academy

Telecom Teams



Telecom Clients

misco
Mawatej Information Systems Co.

القوات الجوية الملكية السعودية

Telecom Partners

SERVICES >

Datacenter Critical Facility

- Cooling Solutions
- Powering Solutions
- Cabinet Solutions
- White Space Planning
- Low Current Solutions
- physical Security Solutions
- Fire suppression Solutions

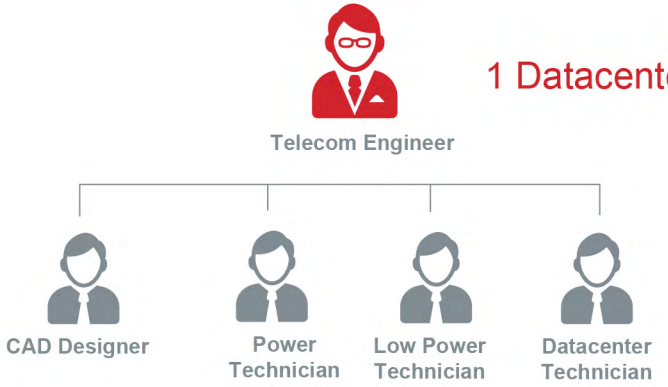




Datacenter References

Project Name	End User
HQ 5 Datacenters Preparation	Military Industries Corporation
Bisha Datacenter Preperation	Ministry of Transportation
Comm. Room Preparation	University of Hail
Comm Room Preparation	Royal Saudi Air force

Datacenter Teams



1 DatacenterTeam

1 Low Power Technician
1 Power Technician
1 electromechanical Technician
3 CAD Designer

Datacenter Clients

Datacenter Partners

Schneider Electric

RITTAL

PANDUIT®

Converge Network Infrastructure

IP telephony Solutions

Wireless and Wired Network Solutions

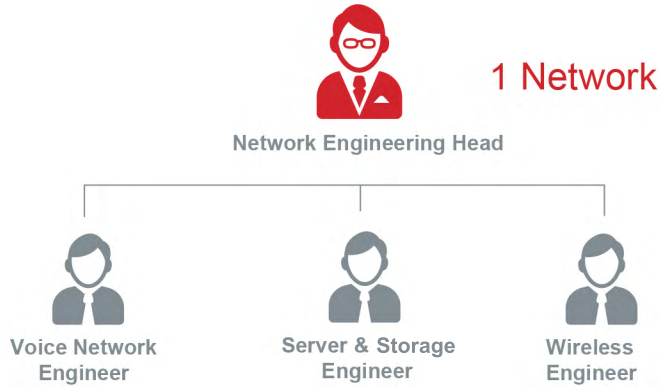
Sorage ans Server Solutions

Visualization Solutions

Converged Network References

Project Name	End User
IP Telephony Upgtade	Military Industries Corporation
Network Connectivity Phase 2	Royal Saudi Air Force
Wireless Connectivity HQ-Bisha	Ministry of Transportation

Converged Network Teams



1 Network Engineering Head

1 Wireless Engineer
2 Server & Storage Engineer
2 Voice Network Engineer

Converged Network Clients

Virtual Network Partners

Symantec Registered Partner

CERTIFICATE OF ACHIEVEMENT

Symantec Corporation is pleased to acknowledge

Integrated Computer Systems

as a Registered Partner in the Symantec Partner Program

September/21/2015

Michael Brown
CEO, Symantec Corporation

Date

TREND MICRO™

Bronze Partner

Integrated Computer Systems

2015

This certifies that the above company has achieved Bronze status in the Trend Micro Partner Program for resellers.

Partha Panda,
VP, Global Channel and Strategic Alliance
Trend Micro
December, 2015

Cisco Channel Partner Program

Premier Certified Partner

CISCO PARTNER
Select Certified

Awarded to

Integrated Computer Systems - ICS

Saudi Arabia

November 2014 - November 2015

AVAYA

أفايا ئي أم ئي ايه لميتد

AVAYA EMEA LTD.
(Saudi Arabian Branch)
P.O. Box 57543 Riyadh 11584
Saudi Arabia
Tel: +966.11.2738100
Fax: +966.11.2008133
www.avaya.ae
C.R.: 1010166598
C.C.R.: 10888

Oct 1, 2015

TO WHOM IT MAY CONCERN

Subject: Avaya Authorized Reseller

This letter hereby certifies that **Integrated Computer Systems (ICS)** is an **authorized partner** in the **Kingdom of Saudi Arabia**.

ICS is appointed to promote solutions offered by Avaya in the areas of Unified-Communication (IPO-based), Data network infrastructure and Video solutions.

This letter is valid for one year from the above date and is renewable on yearly basis. For further inquiries and questions please feel free to contact us.

Sincerely,

Mohamed Abou-Gabal
KSA Country Channel Manager
mogabal@avaya.com

Ref | SA16-443

Strictly Confidential

16th December 2015

Saudi Telecom Company (STC)
Riyadh
Kingdom of Saudi Arabia

Information Technology Sector

Dear Sirs,

We confirm that Integrated Computers Systems company with principal place of business in Zuhair Bin Abi Salma Street, Al Maseef District, Riyadh, Kingdom of Saudi Arabia is an authorised reseller of FireEye's products and services in the Kingdom of Saudi Arabia as of the date hereof.

Please do not hesitate to contact us for any additional Information.

Yours faithfully,

Faysal Makarem
Channel Manager
FireEye, Kingdom of Saudi Arabia

Kingdom Tower
Floor # 28
Riyadh, Kingdom of Saudi Arabia

Mobile: +966 56 643 6522
faysal.makarem@FireEye.com
www.FireEye.com

Safenet UK Ltd Dubai Branch
level 9, Monarch office Tower, One Sheikh Zayed Road
PO Box 333720
Dubai
UAE
Tel : +971 4 3721150
Fax : +971 4 3721151
http://www.safenet-inc.com

5th June, 2013.

To Whom It May Concern.

This is to confirm that Integrated Computer Systems (ICS) based in Saudi Arabia, PO Box 28612, Riyadh 11447 IS the only Senetas Certified Professional Service Partner in Saudi Arabia. Any Senetas procurement within "Saudi Arabia" shall be exclusively done through ICS, till further notice.

Best Regards'
John Doley
Channel Support Manager
SafeNet Inc.

P.O. Box: 333720
Dubai - U.A.E.
SAFENET UK LTD - DUBAI BR.

16 Dec 2015

To Whom It May Concern

RE: Partnership with Integrated Computer Systems

Extreme Networks Middle East hereby states that as of the date of this letter, **Integrated Computer Systems** is an authorized reseller of Extreme Networks in **Kingdom of Saudi Arabia** (the "Authorized Territory").

Integrated Computer Systems has the right to sell Extreme Networks equipment within the Authorized Territory as defined by Extreme according to the terms and conditions of the parties' reseller agreement.

Thank you for considering **Integrated Computer Systems** and Extreme Networks solutions and services.

Sincerely,

Rustam Khametov
Extreme Networks
Channel Manager
Extreme Networks Middle East

Extreme Networks GMEA
Dubai, U.A.E.

PARTNER STORE

Application Confirmation, Enrollment ID 477793

Print

Gold Level Partner, Standard Membership Type

Oracle has received your application. You will receive email communications regarding your application status. If you have questions, you may contact the Partner Business Center.

Application Status

APPROVED

Application Submitted By

Raed Alsweiti

Application Submitted Date

30-SEP-2015

Applicant User Name

raed.alsweiti@ics-saudi.com

Company Registration

Company Name:	Integrated Computer Systems
Phone:	966114943010ext246
Fax:	966114943020
Web Site:	www.ics-saudi.com
Email Address Domains:	@ics-saudi.com
Country:	Saudi Arabia
Address Line 1:	Exit 5

3M Gulf Ltd.

Dubai - UAE
Tel +971 4 367 0777
Fax +971 4 367 0998

P.O. Box 61061
Dubai - UAE
Tel +971 4 883 9266
Fax +971 4 887 1946

Date: 3rd June 2015

To: Saudi Telecom Company

3M - CMD, hereby confirming that, as of the date of this letter, Integrated Computer Systems (**Golden Certified Partner**) and they are participating to get a project .

Name: Tariq Z. Muhanna
Sr. Product Specialist - CMD

Mobile Number: 0546632230
Email: Tzmuhanna@mmm.com

horizon trading est
DIMENSION
مؤسسة بعد الأفق للتجارة

+966 11 454 2377
+966 11 454 2550
info@h-dimension.com

www.h-dimension.com
C.R. 1010235204
P.O.Box 6438 Riyadh 11442
Kingdom of Saudi Arabia

Date: May 10, 2015

TO: SAUDI TELECOM COMPANY

Horizon Dimension Trading Establishment herby confirms as of the date of this letter that Integrated Computer Systems Company (ICS) is a gold certified partner of Horizon Dimension for Multimedia Connect (MMC) passive telecom products (copper, fiber, and cabinet), and they are participating to get projects from the Ministry of Justice in the scope of supplying and installing IT infrastructure solutions.

This letter is issued by us based on our exclusive rights of sales and distribution of MMC products in the area of: **Kingdom of Saudi Arabia.**

Husam Hamad
Mobile: 0540643248

Horizon Dimension Trading Est

MMC
MultimediaConnect
Agence Commerciale :
ZAC des Hauts de Wissous
Bât. Le Cormoran - 3, rue Jeanne Garnerin
91320 WISSOUS
TEL. (+33) 01 69 79 39 80 - Fax (+33) 01 64 48 29 84

MMC MultimediaConnect Exclusive Agent in Saudi Arabia

TO WHOM IT MAY CONCERN

Wednesday, March 18, 2015

INTEGRATED COMPUTER SYSTEMS COMPANY

We would like to confirm that INTEGRATED COMPUTER SYSTEMS COMPANY, based in Saudi Arabia, is accredited as a Palo Alto Networks **'Silver'** partner that matches the following criteria:

- ✓ They are an authorized partner to sell and support the Palo Alto Networks' products and solutions in Saudi Arabia.

This certificate is valid until our next Partner review which will be the 1st of August 2015. Should you require more information, do not hesitate to contact us.

Yours Sincerely,

Jelle Maes
Sales Administration EMEA

Palo Alto Networks Europe, Middle East & Africa
Emiel Banningstraat 47 bus 2
2000 Antwerp - BELGIUM

Certificate of Partnership FY14

Gold Partner

INTEGRATED COMPUTER SYSTEM RIYADH

SAUDI ARABIA

Is an approved member of the **HP PartnerOne program** and qualifies as **HP Gold Partner.**

Gold Partner

HP Gold Partner - PPS Group Hardware

Business Partner

HP Enterprise Business Partner

Gilles Thiebaut
Vice President Indirect Sales
Enterprise Group EMEA Channel

Pierre Jover
General Manager & Vice President
Printing and Personal Systems EMEA Channel

Certificate of Authorized Reseller

Date: 26 May, 2015

Fortinet Singapore Private Limited operates through a channel of independent distributors and resellers. Therefore, Fortinet hereby confirms that: Integrated Compuetr Systems - ICS

Having its registered place of business at:
Al Maseef - Zuhair Bin Abi Salama Street, Riyadh, 11372, SAUDI ARABIA;

is currently an Authorized FortiPartner and is currently authorized throughout SA to sell Fortinet products with the status of a Authorized partner.

This certificate is issued as of the date shown above, and is valid for 180 days from this date.

Provided the FortiPartner identified abovehas purchased applicable support services from Fortinet and the applicable support services have been effectively registered and contracted with Fortinet, Fortinet agrees and undertakes that Fortinet would provide support for the applicable Fortinet products according to the terms of the support agreement, available at https://support.fortinet.com. Fortinet Products are shipped subject to the terms of its then-current End User License Agreement, available at http://www.fortinet.com/doc/legal/EULA.pdf, which sets forth Fortinet's warranty.

This certificate is subject to the FortiPartner maintaining its FortiPartner Agreement with Fortinet and to Fortinet's FortiPartner guidelines. Fortinet's partner program and its guidelines are available for review at http://www.fortinet.com/partners/partner_program/fpp.html. Notwithstanding anything to the contrary herein, authorized FortiPartners do not represent Fortinet and can not make statements that are binding on behalf of Fortinet.

Thomas Schmidt
Associate General Counsel, International
Fortinet Singapore Private Limited
300 Beach Road #20-01, The Concourse, Singapore 199555
Company number 200706224Z

solarwinds

16th September, 2014

Re: Manufacturer Authorization

We, **SolarWinds, Software Europe Limited** (hereinafter "SolarWinds), having an address of Unit 1101, Citygate, Mahon, Cork, Ireland, do hereby authorize: **Integrated Computer Systems Company,** Exit 5 , Hai Elmorooj , Postal Code 11447 P.O Box 28612. (hereinafter the "bidder") to offer all SolarWinds products, of which SolarWinds is the sole manufacturer, for resale or bid on any project in the nation of Saudi Arabia.

We hereby extend to you our full guarantee and warranty in accordance with our own standard End User License Agreement for the products offered and supplied by the above mentioned company. If you have any questions regarding SolarWinds, please don't hesitate to contact us.

Sincerely,

David Owens / Jean Hamilton
Vice President- Finance and Operations - International
DDI: +353 21 500 2905
E-mail: david.owens@solarwinds.com

United States Microsoft.com Home | Site Map

Integrated Computer Systems **Organization Partner ID: 4422814 [Active]** [Sign Out]

Home >> Microsoft Online Services Signed in as Alsweiti, Raed

Microsoft Online Services

Enrollment Status: **Active**
Valid Until: **Sep 15, 2015**

You have completed the requirements to be eligible to receive fees for selling Microsoft Online Services as described in the Microsoft Online Services Partner Agreement. Learn More

Status

Step 1
Enroll in Microsoft Partner Network
View Microsoft Partner Network Agreement. Completed

Step 2
☑ **Agree to terms and conditions of Microsoft Online Services Partner Agreement**
View Microsoft Online Services Agreement Completed

Step 3
Complete the required Tax and Banking Documentation
View and complete documentation required for your region
Note: If you are a U.S. partner or your Online Services customers are in the U.S., you are required to submit a tax form to receive advisor fees.

Step 4
Optional: Associate with a Cloud Channel Developer Distributor
Cloud Channel Developer Distributors provide you with readiness, sales training and account management.
You are currently not associated with a Cloud Channel Developer Distributor.

Select

Display Your Company in Online Directories
This is required so that customers can add you to their subscriptions purchases. Edit your profile here.

The following resources will help you activate your company as you sell Microsoft Online Services

McAfee Ireland Ltd. Building 2000, City Gate, Mahon, Cork, Ireland

18th September 2014

McAfee
An Intel Company

McAfee SecurityAlliance Accreditation – Partner Status

McAfee Ireland Limited hereby confirms that, as at the date of this letter, **integrated computer systemsICS** with offices located at **exit 5, Riyadh, 11447, Saudi Arabia** is an **Associate level partner.**

At this level, the partner has access to the McAfee eLearning certifications and has access to re-sale of **Open Resale** products

Available Products	
Open re-sale (no authorization required to sell)	Partners may distribute the McAfee products and services as identified in the then current McAfee price book, as updated from time to time, excluding those products flagged as requiring Authorization (to sell) within the McAfee price book available from authorized distributors.
Closed re-sale (authorization required to sell)	Authorized Partners may distribute the McAfee products and services as identified in the then current McAfee price book, as updated from time to time, including those products flagged as requiring Authorization (to sell) within the McAfee price book available from authorized distributors.

All McAfee Software is subject to McAfee End User license Agreement (EULA) and all McAfee Support and Services are subject to respective McAfee standard terms.

For the avoidance of doubt, **integrated computer systemsICS** is an independent entity that acts in its own name and account and is not entitled to represent McAfee in any way or make statements on McAfee's behalf.

Sincerely,

Vice President Channels & Commercial Sales EMEA

JEPPESEN
A BOEING COMPANY

55 INVERNESS DRIVE EAST
ENGLEWOOD, CO 80112

TEL 303.799.9090
FAX 303.328.4153

JEPPESEN.COM

Mr. Raed Alsweiti
Technical Proposal Manager
Integrated Computer Systems
Riyadh, Saudi Arabia
+966-533-536-911

September 16, 2014

Re: Possible Navigation Data File Services from Jeppesen to Support the Royal Saudi Air Force

Dear Mr. Alsweiti,

Please be advised that provided that the RSAF selects your company for the above service as a vendor and that your company meets all the criteria of requirements set forth by Jeppesen and has been cleared and approved by our Legal & Contracts Department, we have no issue getting under a contractual agreement inclusive of Jeppesen's accepted Terms and Conditions.

The RSAF must notify my office officially and in writing of their decision to make you the sub-contractor for Jeppesen services in the future.

Should you have any questions or concerns, please don't hesitate to reach out to me.

Sincerely,

Ala Khalaf
Sales and Service Director, Middle East
Government & Military Aviation

AccessData

ACCESSDATA PARTNER AGREEMENT

This AccessData Partner Agreement (including any appendices, schedules and exhibits hereto, the "Agreement") is made as of the 16th of September, 2013 ("Effective Date") by and between AccessData Corporation Limited, a private limited company registered in England & Wales and wholly owned subsidiary of AccessData Group, Inc. (Delaware, USA), with offices located at 1 Bedford Street, London, WC2E 9HG (together with its successors, subsidiaries, affiliates or assigns, "AccessData") and Integrated Computer Systems (ICS), a Saudi Arabian company with offices located at 75 Zuhair Bin Abi Salama Street, Riyadh, Saudi Arabia ("Partner").

WHEREAS, AccessData develops and manufactures software and provides services, support and training related to that software;

WHEREAS, Partner will, subject to the terms and conditions of this Master Agreement and the relevant Appendices, supply the services detailed in the following Appendices:

Appendix A. Reseller Agreement

NOW, THEREFORE, in consideration of the mutual benefits of the covenants and restrictions herein contained, AccessData and Partner agree as follows:

Section 1. Definitions

1.1. "Advanced Product" means the AccessData Software products AD Lab, AD Enterprise, AD eDiscovery, AD ECA, Summation, SilentRunner, CIRT and any other enterprise-level Software product permitting the simultaneous use and collaboration of two or more Named Users / Customers.

1.2. "Appendix" and "Appendices" mean the additional terms and conditions detailing portions of the business relationship between the parties, appended to this Agreement and incorporated by reference above and by Section 13.2 of this Master Agreement.

1.3. "Confidential Information" means all information, whether commercial, financial, technical or otherwise, whether or not disclosed by one party to the other party, which information may be contained in or discernible from any form whatsoever (including oral, documentary, magnetic, electronic, graphic or digitised form or by demonstration or observation), whether or not that information is marked or designated as confidential or proprietary, and all matters arising prior to or during the term of this Agreement, including but not limited to all Advanced Product(s), Intellectual Property, hardware, software, information belonging to or in respect of AccessData or Partner (or any of their affiliates) and/or any of their customers or suppliers, which relates to any research, development, trade secrets, know-how, ideas, concepts, formulae, processes, designs, specifications, past, present and prospective business, current and future products and services, internal management, information technology and infrastructure and requirements, finances, marketing plans and techniques, price lists and lists of, and information about, customers and employees, and all materials and information belonging to third parties in respect of which either party (or any of their affiliates) or any of their customers or suppliers owe obligations of confidence.

1.4. "Customers" means the individuals or entities that (i) purchase a license to the Software from Partner for their own internal business use, (ii) enter into a Hosting and/or Services agreement with Partner, (iii) purchase Training from Partner, and/or (iv) have received and agreed to AccessData's then current Software license agreement.

1.5. "Customer Content" means any and all material or data (which may or may not contain Personal Data) provided by Customer, including but not limited to case-related data in any paper or electronic format, Customer work product or reports created in or uploaded to the Software, and Customer owned or provided data collected by or for Use in the Software.

1.6. "Documentation" means any operating manuals, user instructions, technical specifications or

AccessData

ACCESSDATA PARTNER AGREEMENT

APPENDIX A
RESELLER AGREEMENT

WHEREAS, AccessData develops and manufactures software Products;

WHEREAS, Partner is in the business of selling products similar to that developed and manufactured by AccessData; and

WHEREAS, Partner desires to sell AccessData's Products subject to the terms and conditions of this Reseller Agreement.

NOW, THEREFORE, in consideration of the mutual benefits of the covenants and restrictions herein contained, AccessData and Partner (for the purposes of this Appendix, "Reseller") agree as follows:

Section 1. Authorization and Territory

1.1 Grant and Acceptance: AccessData hereby grants and Reseller hereby accepts a non-exclusive, non-transferable right to promote, market, and sell the Products in the Reseller Territory (as defined below) pursuant to the terms and conditions of this Appendix A and the Master Agreement (this Appendix A and the Master Agreement being this "Reseller Agreement").

1.2 Non-Exclusivity: Absent written agreement between the parties, AccessData reserves the right to increase the number of resellers of the Products in the Reseller Territory or elsewhere and to sell the Products to any person or entity, using other resellers or its own personnel or independent sales representatives, without obligation or liability of any kind to Reseller.

1.3 Territory: Reseller's distribution of AccessData Products under the terms of this Appendix is restricted to the following regions: Saudi Arabia.

Section 2. Term and Renewal

2.1 Term and Renewal: The term of this Reseller Agreement shall begin on the Effective Date, and shall renew automatically on the anniversary of the Effective Date for successive one-year periods thereafter (each a "Year"), unless terminated in accordance with Section 8 of the Master Agreement.

Section 3. Order, Pricing and Shipment of Products

3.1 Order Procedure: Reseller shall place all Orders for Software, Support, Services or Training by submitting a Reseller Order Form attached herein as **Schedule 1** to this Appendix to Reseller's regional AccessData Account Executive or Internal Sales Representative (collectively, "Sales Representative"). Orders may be placed with Reseller's Sales Representative by direct email to that representative or by general email to sales@accessdata.com (for the United States) or internationalsales@accessdata.com (outside of the United States).

3.2 Pricing: Reseller can place Orders at the AccessData Authorized Reseller pricing as listed below. Software Orders can be placed at a discounted rate of 15% off the Suggested Retail Price ("SRP"). Support and Training Orders can be placed at a discounted rate of 5% off the SRP. Services Orders can be placed at a discounted rate of

5% off the SRP. Current pricing will be provided to Reseller on a quarterly basis or upon request by the AccessData International Partner Manager. Current pricing will be provided to Reseller upon request to the AccessData International Partner Manager or via email to partnerinfo@accessdata.com.

3.3 Annual Target: The Reseller discounts specified in Section 3.2 of this Reseller Agreement will be maintained providing the agreed revenue target of $250,000 USD is met by Partner during each Year of this Reseller Agreement; however, if during any Year, Reseller should surpass the agreed revenue target or fails to track against the agreed target, then margins will be reviewed on a quarterly basis.

3.4 Customer Prices: Reseller shall have the right to set the prices for Software sold by Reseller to Customers, provided the current SRP is not exceeded.

3.5 Shipping Procedure: Except as otherwise agreed by AccessData and Reseller, AccessData shall provide to Reseller a physical or virtual license key for each ordered Product within 48-hours of receiving Reseller's order, together with any applicable Media, Documentation, hardware or other Product materials. If not specified in Reseller's order, AccessData shall select the mode of shipment and the carrier. For any physical shipment, title and risk of loss or damage to the Products in transit shall pass from AccessData to Reseller when the Products leave AccessData's premises.

3.6 Documentation: Each shipment shall include a shipping order. The price, applicable discounts, shipping and handling fees, and all applicable taxes and duties will be sent under separate cover. AccessData shall also provide to Reseller a monthly statement of account listing all Orders shipped, payments made, and credits given since the date of the previous month's statement when there has been activity on the account in the prior thirty (30) days.

3.7 Products Non-Returnable: All Orders are final upon shipping. AccessData will not be required to accept the return of Orders, except as allowed under Section 6 of this Reseller Agreement.

3.8 Product Obsolescence: AccessData agrees to notify Reseller that a Product will be replaced with an updated version. Reseller shall have the right to return any obsolete Product for full credit towards the purchase of other AccessData Products.

Section 4. Payment Terms

4.1 Payment: For the purposes of this Appendix and in accordance with Section 3.1 of the Master Agreement, Reseller shall pay for all Orders in USD or EUR currency via wire transfer.

4.2 Credit: Reseller must pay for any Order in full at the time of placing the Order or upon providing AccessData with a letter of credit from a reputable financial institution. AccessData reserves the right to withhold future Orders until all Orders are paid in full, as well as the right to refuse any Order if significant credit concerns arise.

4.3 Customer Payment and Terms: Reseller shall have the right to set terms for payment by Customers to Reseller for all Products ordered by the Customer. Any such Customer payment terms shall be without prejudice to and shall have no effect on Reseller's payment obligations to AccessData pursuant to this Reseller Agreement.

Section 5. Reseller's Responsibilities

5.1 Sales Effort: Reseller shall use its best efforts to promote the sale and distribution of the Products and shall utilize its own facilities and personnel to their full potential in that regard. Reseller shall not subcontract its rights under this Reseller Agreement or subordinate its sales efforts to a third party that is outside this Reseller Agreement.

5.2 Product Procurement Instructions: Before any Advanced Product sale is made, Reseller shall notify its regional AccessData Sales Representative of the potential sale in order to permit AccessData reasonable time and opportunity to negotiate a signed Software licensing agreement with the Customer. AccessData (a) must approve in advance and in writing any Advanced Product procurement or licensing agreement which AccessData may enter into with Customers and (b) shall not be subject to the terms or conditions of any agreement that conflicts with AccessData's preferred Software license agreement or is not otherwise approved in writing by AccessData. Reseller has no right to modify such agreements between Customers and AccessData or otherwise bind AccessData to any terms or conditions not approved by AccessData in writing.

Section 6. Limited Warranty to Reseller

6.1 AccessData Limited Warranty: In addition to the terms of Section 6 of the Master Agreement, AccessData warrants to Reseller that the Products are free from manufacturing defects under normal use for ninety (90) days from the date of receipt of the Product by a Customer ("Warranty Period"). In the event a Product is returned to AccessData during the Warranty Period for failure to meet this warranty, AccessData shall replace the defective Product at no cost to Reseller. AccessData shall pay standard non-couriered freight charges incurred by Reseller in returning defective Products and all costs of shipping replacement Products to Reseller (or, if Reseller designates, directly to Customers). Reseller shall be solely responsible for warranty obligations to Customers, in which AccessData as the manufacturer will take responsibility for warranty as long as the Customer qualifies as an actual AccessData End User. The warranty given by AccessData pursuant to this Section 6.1 shall be void and AccessData shall have no obligation or liability under this Section 6.1 if Reseller in any way modifies or expands AccessData's obligations to the Customers.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement by their duly authorized representatives as of the respective dates indicated below.

INTEGRATED COMPUTER SYSTEMS (ICS)	**ACCESSDATA CORPORATION, LIMITED**
By: Karajih	**By:** DocuSigned by: Tim Leehealey 2914938F91464BD...
Name: Dhia M. Karajih	**Name:** Tim Leehealey
Title: Vice President, Sales and Operations	**Title:** CEO
Date: 16 Sep, 2013	**Date:** 9/23/2013

ORACLE
PARTNERNETWORK

Specialized. Recognized by Oracle.
Preferred by Customers.

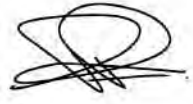
This certifies that

Integrated Computer Systems

has achieved the level

ORACLE **Gold Partner**

Penny Philpot
Group Vice President,
Worldwide Alliances & Channels,
Partner Services



This annual partnership is currently valid until

30-Sep-2017

المملكة العربية السعودية
وزارة الشؤون البلدية والقروية
وكالة الوزارة لشؤون تصنيف المقاولين

وزارة الشؤون البلدية و القروية
Ministry Of Municipal & Rural Affairs

الرقم ١٧٧٧٢
التاريخ ١٤٣٨/١٠/١٦
رقم الملف ١٦٨٦٤

شهادة تصنيف المقاولين

رقم ٢٠٧٧٨

اسم المقاول : شركة المترابط لأنظمه الحاسب الألي الجنسية : سعودية
نوع الملكية : شركة ذات مسؤولية محدودة

رقم السجل التجاري : ١٠١٠١٧٤٣٩٤ تاريخه : ١٤٢٢/١٢/٢٢ مصدره : الرياض
العنوان : ص . ب ٢٨٦١٢ الرياض ١١٤٤٧ فاكس : ٠١١٤٩٤٣٠٢٠ هاتف : ٠١١٤٩٤٣٠١٠

مجال التصنيف	الدرجة
الاعمال الالكترونية (تركيب أجهزة الحاسب الآلي والشبكات)	الثانية
تقنية الإتصالات (تركيب أجهزة الاتصالات السلكية واللاسلكية وتطوير نظم وبرامج الاتصالات وشبكات الانترنت)	الثانية

(مصنف في مجالين فقط)

تنتهي صلاحية هذه الشهادة بتاريخ : ١٤٤٢/١٠/١٦ هـ

وكيل الوزارة لشؤون تصنيف المقاولين

عبدالرحمن بن محمد المفرج

وزارة الشؤون البلدية والقروية
وكالة شؤون تصنيف المقاولين
إدارة خدمات المقاولين

ملاحظة هامة جداً : يجب مطابقة الصور على الأصل في كل حالة .
كل كشط أو تغيير في هذه الشهادة يلغيها .

مصلحة مطابع الحكومة - ٣٨٢٩٧٩

Certificate of MemberShip

شهادة الاشتراك

القطاع التنفيذي
الإدارة العامة لخدمات الإشتراكات
إدارة شئون العضوية

Unified Membership No. : 101000 **119733**

رقم العضوية الموحد : ١٠١٠٠٠١١٩٧٣٣

Date of Issue : **29/12/2015**

تاريخ الأصدار: ٢٠١٥/١٢/٢٩

Classification : **Second**

الدرجـــــــة: الثانية

Riyadh Chamber of Commerce and Industry certifies that:

تشهد الغرفة التجارية الصناعية بالرياض بأن :

ALMTRABET EST. FOR COMPUTER SYSTEMS.

شركة المترابط لانظمه الحاسب الالى

Commercial Register No 1010174394

المقيدة بالسجل التجاري / الترخيص رقم ١٠١٠١٧٤٣٩٤

The Certificate expires on 30/11/2020

وينتهي سريان هذه الشهادة في ٢٠٢٠/١١/٣٠م

ص. ب: 28612 الرمز: 11447 هاتف: 4943010 فاكس: 4943020

مدير عام خدمات العملاء

ختم الغرفـــة

اي كشط او تعديل في هذه الشهادة يلغيها

بسم الله الرحمن الرحيم

المملكة العربية السعودية
وزارة المالية
مصلحة الزكاة والدخل

(١٨٥)

فرع الرياض

1020029612

رقم الشهادة : ١٠٢٠٠٢٩٦١٢
التاريخ : ١٤٣٧/٠٨/١٥هـ

الرقم المميز : ٣٠١٠٦٧٥٩٩٧

شهادة

تشهد مصلحة الزكاة والدخل بأن المكلف / شركة المترابط لأنظمة الحاسب الآلي
وسجل تجاري رقم ١٠١٠١٧٤٣٩٤
قدم إقراره عن الفترة المنتهيه في ٢٠١٥/١٢/٣١ م
وقد منح هذه الشهاده لتمكينه من إنهاء جميع معاملاته بما في ذلك صرف مستحقاته النهائية عن العقود.
يسري مفعول هذه الشهادة حتى تاريخ ١٤٣٨/٠٨/٠٤ هـ الموافق ٢٠١٧/٠٤/٣٠م.
(الرابع من شعبان ألف و أربعمائة و ثمانية و ثلاثون هجري)

الختم الرسمي

الوظيفة : مدير عام فرع المصلحة بالرياض المكلف
الاسم : خالد عبيد حماد الظاهري
التوقيع :

مصلحة الزكاة والدخل
١٣٧٠ هـ
فرع الرياض

CERTIFICATE

This is to Certify that the
Environmental Management System
of

Integrated Computer Systems.

AL MASIF , EXIT 5 , ZUHAIR BIN ABI SALMA STREET , RIYADHKINGDOM OF SAUDI ARABIA

has been independently assessed and is compliant with the requirements of

ISO 14001:2015

This Certificate is applicable to the following product or service ranges:

Providing Security Solutions , Structured Cabling , Networking , Data Center Solutions ,Operation & Maintenance and System Integration Services

:: Certificate No :: 108525-A02

Date of initial registration	**03 April 2017**
Surveillance audit on or before	**29 March 2018**
Certificate expiry	**02 April 2018**
Recertification Due	**02 April 2020**

This Certificate is property of LMS Certifications and remains valid subject to satisfactory surveillance audits.

Director

Accreditation

CB-006-MS

LMS Certifications Private Limited
1-Ananddham, Opp. Kukrail Picnic Spot Gate,
Faridi Nagar, Lucknow - 226015, UP, (INDIA).
e-mail :- info@lmsassessment.com,
Visit :- www.lmsassessment.com.

CERTIFICATE

This is to Certify that the
Occupational Health & Safety Management System
of

Integrated Computer Systems.

AL MASIF , EXIT 5 , ZUHAIR BIN ABI SALMA STREET , RIYADHKINGDOM OF SAUDI ARABIA

has been independently assessed and is compliant with the requirements of

OHSAS 18001:2007

This Certificate is applicable to the following product or service ranges:

Providing Security Solutions , Structured Cabling , Networking , Data Center Solutions ,Operation & Maintenance and System Integration Services

:: Certificate No :: 108525-A03

Date of initial registration	**03 April 2017**
Surveillance audit on or before	**29 March 2018**
Certificate expiry	**02 April 2018**
Recertification Due	**02 April 2020**

Director

Accreditation

DAC

CB-106-MS

LMS Certifications Private Limited
1-Ananddham, Opp. Kukrail Picnic Spot Gate,
Faridi Nagar, Lucknow - 226015, UP, (INDIA).
e-mail :- info@lmsassessment.com,
Visit :- www.lmsassessment.com.

BSCIC Certifications Pvt. Ltd.

Certificate Of Registration

QUALITY MANAGEMENT SYSTEM

This is to certify that:

ICS (INTEGRATED COMPUTER SYSTEMS)

AL MASIF, EXIT 5, ZUHAIR BIN ABI SALMA STREET
RIYADH, KINGDOM OF SAUDI ARABIA

Hereby granted the Certificate Number : BN16147/16014

Subsequent to the **Assessment** of the organization and has been found to be operating a Quality Management System which complies with the requirements of

ISO 9001:2015

For the following scope :

Providing Security Solutions, Structured Cabling, Networking, Data Center Solutions, Operation & Maintenance and System Integration Services

Originally Registered: **14-Mar-2017** Latest issue: **14-Mar-2017** Expiry Date: **13-Mar-2020**

For BSCIC CERTIFICATIONS PVT.LTD.

Sanjay Seth
Managing Director

Validity of this Certificate is subject to Annual Surveillance Audits to be done Successfully on or before 14-Mar-2018 and 14-Mar-2019 resp. (In case if Surveillance Audit is not allowed to be conducted; this Certificate shall be Suspended/Withdrawn).

Please re-check the validity thereafter at http://bscic.com/admincontrol/certificatestatus.php or www.bsc-icc.com at REGISTRATION STATUS.This Certificate of Registration is granted subject to relevant provisions of the BSCIC Certifications PVT. LTD. Contract Terms & Scheme for Registration Form B018 (Latest Version). Please see B 018 at our website www.bsc-icc.com.The certificate of Registration remains the property of BSCIC Certifications Pvt. Ltd. and shall be returned immediately upon request. BSCIC Headquarters: IInd Floor, SCO 150, Sector - 21 C, Faridabad 121001 Haryana, INDIA

BSCIC JAS-ANZ www.jas-anz.com.au/register ISO 9001 REGISTERED

INTEGRATED COMPUTER SYSTEMS

شركة المترابط لأنظمة الحاسب الآلي

Integrated Computer Systems

75, Zuhair Bin Abi Salma St., Al Maseef Dist.,
Riyadh, Kingdom Of Saudi Arabia
P.O.Box. 28612 Riyadh 11447

+966 11 494 3010
+966 11 494 3020
info@ics-saudi.com

www.ics.sa