EUROPEAN DYNAMICS' MANAGED APPLICATION SERVICES

SERVICE DEFINITION

TABLE OF CONTENTS

1 Introduction 1
2 High-level description of the service 1
2.1 The EDMAS service 1
2.2 Principles 2
2.3 Services 3
2.4 Sites 3
3 Infrastructure 3
3.1 Hardware 3
3.2 Software 4
3.3 Network 4
3.4 Fail-over Strategy 5
3.4.1 Overall Availability 5
3.4.2 Service Availability 5
3.4.3 Capacity Management 6
4 Services 7
4.1 On Boarding / Off Boarding 7
4.2 Service constraints 7
4.3 Service Levels 7
4.3.1 Information Assurance 7
4.3.2 Service Levels – System 7
4.3.3 Service Management Details 8
4.3.4 Adherence to the EU Code of Conduct 9
4.3.5 Service Levels – Help Desk 9
5 Contractual matters 10
5.1 Pricing Overview 10
5.1.1 Volume Discounts 10
5.1.2 Data Extraction Costs 11
5.1.3 Data Restoration / Service Migration 11
5.2 Ordering and invoicing 11
5.3 Termination of contract 11
5.3.1 Termination by Customers 11
5.3.2 Termination by Supplier 11
5.4 Technical requirements 11
6 Business continuity and disaster recovery 12
6.1 Business Continuity 12
6.1.1 Business Continuity Policy 12

6.1.2 Disaster Recovery Plan 12
6.2 BCDR Objectives 13
6.2.1 Triggers for Activation 14
6.2.2 High Availability (HA) 14
6.3 Disaster Recovery 14
6.3.1 Disaster Recovery Site (DRS) 14
6.3.2 Restoration of primary site 14
6.3.3 Recovery processes 15
7 Backup and restoration 15
7.1 Backup and Recovery Policy 15
7.1.1 Backup System Infrastructure 16
7.1.2 Other Provisions 16
8 Service monitoring 16
8.1 Monitoring Tools 16

1 Introduction

The service is offered by EUROPEAN DYNAMICS (https://www.eurodyn.com). The EUROPEAN DYNAMICS group of companies (ED) is a leading Information Technology and Telecommunications services provider with a long involvement in the delivery of IT projects and the provision of IT support services for European Institutions and other international and government organizations in the EU and worldwide. ED is headquartered in Luxembourg, with branch offices in Athens (Greece), Brussels (Belgium), London (UK), Basel (Switzerland), Berlin (Germany), Vienna (Austria) and The Hague (the Netherlands). EUROPEAN DYNAMICS UK LTD belongs to the ED group and offers all ED services in the UK in collaboration with other ED companies. All companies in the group share resources, management and infrastructure, which ensures a common customer interface.

EUROPEAN DYNAMICS is proud to make available on G-Cloud its modern and secure server infrastructure that offers an excellent environment for any type of enterprise services conducted by its customers. The EUROPEAN DYNAMICS' Managed Application Services (EDMAS) offer a virtualised environment either as an Infrastructure-as-a-Service (IaaS) or as a Platform-as-a-Service (PaaS) configuration.

In the IaaS model, the Customer is offered a virtual server, storage, and networking environment that provides full freedom in the choice of the operating system and system software to deploy on it. The PaaS model includes the IaaS components and additionally the operating system and optionally other system software components, such as application servers, web servers, database management systems, etc. all managed by the Service Provider.

The offered IaaS/PaaS solutions provide the hardware, system software and networking environment that will allow easy deployment of software systems that depend on a range of popular infrastructure options. The platform provides the necessary security that contributes towards UK GDPR compliance of the services operating using EDMAS.

2 High-level description of the service

2.1 The EDMAS service

The Service Provider has implemented EDMAS as an IaaS/PaaS platform, on which Software as a Service (SaaS) solutions can operate. The EDMAS platform is geared at delivering elevated levels of security, availability, and performance to SaaS customers.

EDMAS is provided as a secure, available, hosted, managed service that is accessed by customers via the internet. In addition to the information processes that each software system facilitates, a range of core services including help desk, system management monitoring and support services are provided to customers as sub-systems of an overall Managed Application Services system delivered as a single unified solution to address Customer requirements.

ED manages its own datacentre and hosts EDMAS services on a dedicated infrastructure platform collocated in Athens, Greece. The datacentre provides state-of-the-art hosting facilities located in a highly secure environment near key IT service and communication providers operating in the region. To provide reliable Managed Application Services meeting the SLA, all critical infrastructure components are configured with full redundancy.

The EDMAS service has the following features:

- Redundant hardware configurations that allow operation under the Tier-3 specification. Redundancy extends to all server, storage, networking, power, air conditioning and connectivity aspects of the service.
- Implementation of the Disaster Recovery (DR) site at a different geographical location approx. fourteen miles away from the primary data centre. The primary and the DR sites are connected through private high-speed dedicated lines that ensure fast failover performance.
- System architecture is based on industry standard best of breed HPE enterprise server and storage solutions that in combination with VMWare virtualisation software enable fast provisioning of virtual servers tailored to the requirements of the Customer.
- Enhanced physical and logical security that allows meeting strict security requirements.
- Redundant storage implemented using HPE enterprise storage solutions that allow easy provisioning of storage with high availability and performance characteristics.
- Industry standard backup/restore mechanisms that can operate at the physical, logical and filesystem level as required.
- Encrypted storage that ensures compliance with privacy requirements at the infrastructure level.
- VPN and VLAN technologies that allow customised network configuration to meet our customers' security requirements.
- Highly trained and security-cleared personnel that ensure continuous operation and substantial Customer support in line with the applicable SLAs.

The environments are based on HPE Compute Servers combined with VMware virtualisation software to provide a high performance and a highly scalable Managed Application Services platform. The EDMAS service maintains an ISO27001:2013 certification.

Detailed information about the components comprising the Service Provider's hosting infrastructure and network topology is provided in the following sections.

2.2 Principles

EDMAS delivers managed services for ED customers. Such services are offered in strict compliance to the most efficient methodologies known today in the market (e.g., ITIL) and include all necessary support of the IT and telecom systems offered; 1st, 2nd and 3rd level support to users and administrators of specific applications; and provision of Managed Application Services.

The infrastructure meets the principles of:

- **Security**: Infrastructure and services are operated under ISO 27001:2013 incorporating an end-to-end security model that protects from malicious attacks/theft. The platform undergoes regular, independent technical and procedural auditing.
- **Scalability** to support growing user & business demand. Scalability is achieved vertically (components scale up) and horizontally (infrastructure scales up).
- **High Availability** (HA) is achieved by:
  - ◊ HA components at every point of the infrastructure, minimising component errors (e.g. components with high MTBF, dual paths, hot swap, and redundancy).
  - ◊ Internet connectivity, redundant lines from two independent ISPs.
  - ◊ Eliminating single points of failure with two or more components in all service tiers.
  - ◊ Providing dual paths for all network connections ensuring always up connectivity.
  - ◊ Reverting to DR site promptly, according to the Business Continuity Policy (BCP).

2.3 Services

As part of the service we make use of our extensive experience in the provision of maintenance and operation services, concerning software applications and hardware systems. The maintenance and support services include:

- Customer support, including hot-line support, remote problem diagnosis and support, on-site support.
- Disaster recovery and back-up plan.
- System administration and operation.
- Control measures.

We have established a Customer Support Centre (CSC) to provide technical support to our customers. Access modes of the CSC include phone, e-mail, and fax. The response is direct, because the company operates a special centre for problem announcements, the Single Point of Contact (SPOC). As soon as the problem is registered in the helpdesk system a trouble ticket is assigned to the problem. The CSC has the responsibility for all the control functions and procedures required ensuring integrity of service and responsiveness to customer incidents and requests. The employed methodology follows ISO 9000, ITIL and industry best practices that have been established after many years of experience within the company.

2.4 Sites

Two High Security & High Availability Datacentres are used:

- Primary: ISO 27001 & ISO 9001 Tier III datacentre collocated at Metamorfosis II, TI Sparkle Greece, Athens.
- DR: ISO 27001 Tier III datacentre collocated by TI Sparkle Greece S.A. (subsidiary of Telecom Italia) at 25 Km distance from the primary site.

3 Infrastructure

3.1 Hardware

EDMAS environments (e.g. development, production) are separated from each other as well as from other systems hosted in the datacentre. The infrastructure supports edge segmentation/virtualisation for network, security, and storage. Environments are separated by firewalls filtering network traffic. A dedicated Storage Area Network (SAN) provides HA storage to the production environment, separate (not shared) from corporate SAN.

ED provides the service on a server farm consisting of 32 **Compute Servers.**

The server farm hosts multiple virtual servers per compute server using VMware. They have adequate processing and memory capacity to accommodate current and future requirements.

The SAN comprises multiple Enterprise Grade storage arrays (**HPE Primera, HPE NIMBLE, HPE 3PAR)** providing an aggregated raw capacity of 1PB. SAN connectivity is provided via a network of redundant fibre channel switches.

The **HPE StoreOnce Appliances (5100 and 4500)** are backup/recovery appliances providing disk-based, encrypted backup and de-duplication functionalities. HPE StoreOnce Appliances delivers a scalable solution between 48-216TB. The appliances meet backup windows with speeds of up to 14TB/hour using HPE StoreOnce Catalyst.

3.2 Software

EDMAS services are hosted on VMware cluster-based environments primarily using **Red Hat Enterprise Linux**. Red Hat Enterprise Linux is deployed and configured according to the instance's functional role (e.g. web, application, and database).

The solution comprises four components: virtualisation software (**VMware VSphere Enterprise Plus**), compute servers, SAN storage and Gigabit Ethernet switches.

Scalability and the reduction of financial overheads are achieved by applying:

- **Server Virtualisation**: The platform uses **vSphere Distributed Resource Scheduler** to meet peak service demands by automatically distributing loads across the server pool. Capacity increase is achieved by adding blades to the pool on-the-fly.
- **Storage Virtualisation**: The SAN provides high performance and tiered storage. It virtualises physical storage which is offered to the servers. Storage resources are thin-provisioned, formatted as VMware VMFS. By combining thin provisioning with VMFS existing storage is used and additional storage on-the-fly is offered.
- **Capacity Management** is provided through VMware tools and dedicated software such as **Nagios** & **LibreNMS**, which help tracing bottlenecks and performance trends.
- **Application-level Scalability**: The platform facilitates rapid provisioning of resources to achieve horizontal and vertical scaling of infrastructure. The application layer employs load balancing and clustering to support growing user needs and business requirements.
- **High Availability** for applications running in VMs is provided by **VMware HA**. The ESX servers are clustered using a shared resource pool. VMware HA monitors all hosts in the cluster. If one fails, it immediately restarts the affected VM on a different host.

3.3 Network

The network implementation of EDMAS is designed for HA with a layered architecture. EDMAS environments are connected to the backbone network as separate environments through a carrier grade high-performance firewall system (2 **Fortinet Fortigate 1800F Next Generation Firewalls)** in an active-standby state-full failover mode for HA. Fortigate NGFWs prevent malware and attacks using Intrusion Prevention System (IPS). They are licensed with FortiGuard Unified Threat Management (UTM) Protection which includes Application Control, IPS, Web Filtering, AntiVirus, AntiSpam and IP/Domain Reputation.

The internal core network is fully redundant, consisting of 2 **HPE Data Center Switches** implementing a Terabit backbone. Independent logical networks within the physical network are supported by VLANs on Catalyst switches.

VLANS are used to separate the business units into zones (e.g. development, management, helpdesk, and user). Inter-VLAN routing is implemented through firewalls. VLANs are a critical component of access control and combined with Access Control Lists, which are hardware-processed on Catalyst switches, forming the basis of a security-in-depth network design.

Load balancing devices **(F5 BIGIP Virtual Appliances**) are configured as a redundant cluster that provides HA clustering, Web Application Firewalling, Content Management and SSL termination of incoming web traffic to the EDMAS platform.

Internet connectivity of the primary datacentre consists of two independent ISPs for HA with independent fibre carriers, providing multi-gigabit throughput each.

The redundant Internet connections include:

- A Tier 1 Internet Circuit from Sparkle TI Greece.
- A Tier 1 Internet Circuit from Cosmote (member of the OTE Group, a Deutsche Telecom company, and incumbent telecommunications services provider of Greece, which includes OTEGLOBE, a Tier 1 provider).

3.4 Fail-over Strategy

3.4.1 Overall Availability

EDMAS services are hosted on HA infrastructure, with all components in a fully redundant active-active configuration. The hosting platform ensures no single point of failure. By using only HA components (components with high MTBF, dual paths, hot-swap options, redundant options) errors are minimised. Therefore, we guarantee and exceed 99.9% availability.

The service platform is clustered at all layers (redundant network/storage paths and SAN/network devices, clustered physical servers, dual controller storage, application/database, and OS clustering). The likelihood of an unplanned service downtime is minimal. This is backed up by the overall uptime over the last 3-year period for all internally hosted instances. The achieved availability is above 99.99%.

The key redundancy elements of the Managed Application Services platform are:

- **Redundant SAN** with redundant fibre switches and enterprise-grade storage arrays using redundant controllers and redundant disks, RAID 5 and 6.
- **Redundant power**: All equipment has redundant power feeds from a dual UPS backed up by redundant diesel generators.
- **Redundant network** including firewalls, switches, and routers with automatic failover mechanisms.
- **Multiple Internet connections** configured as simultaneously active (BGP-advertised) ensure seamless continuity of Internet access if one of the circuits fails.
- **Server & storage redundancy**: The servers and storage are designed for HA and implemented as a cluster of physical server and storage components.
- **Virtualisation clustering**: VMware HA software is deployed to virtualise and cluster OS environments over the physical clusters of Compute Servers.
- **Database clustering**: Database Services are clustered over multiple OS instances, thus providing full redundancy and availability.
- **Application-level clustering**: Application layer services are clustered for HA and scale-out performance. Multiple virtualised OS instances running application servers are deployed on the VMware HA server platform.
- **Load balancing and SSL termination redundancy**: A clustered pair of F5 BIG-IP Application Delivery appliances provide SSL termination and load balancing to the application server farm.

3.4.2 Service Availability

We guarantee 99.9% availability with an expectation of 99.99% based on experience. The availability and performance of the system is assured by:

- Continuous and automated monitoring of the service and infrastructure components.
- Systematic performance review and capacity reports.
- Planned maintenance on the Managed Application Service hardware and software components.
- Systematic tuning and optimisation of service components.

3.4.3 Capacity Management

Our Capacity Management (ITIL 2011) determines proactively the Managed Application Service's needs, to ensure sufficiently resourcing and to achieve the required service levels. The addressed areas include:

- **Business**: Ensuring that the future business requirements for IT services are considered, planned, and satisfied promptly. This can be achieved by forecasting future requirements by examining current resource utilisation.
- **Service**: EDMAS services are continuously monitored, ensuring that performance KPIs are maintained, and that data is recorded, analysed, and reported. Preventive actions are taken to ensure service performance.
- **Component**: All components are monitored and collected data is recorded, analysed, and reported. If required, actions are taken to allocate additional resources so that IT services meet the business requirements.
- **Human Resources**: Short- and long-term needs for HR required to provide high quality services.
- **Demand Management**: Manage the capacity when demand is likely to exceed the ability to deliver. It is achieved by assigning resources according to priorities.
- **Application Sizing**: Determine the service level, resource and cost implications of a new application or enhancement to an existing application.
- **Modelling**: Predict the performance/availability of a specified system under a given working volume.

We use monitoring tools (VMware, Cacti) to address capacity issues proactively. The monitored Configuration Items (CI) thresholds are defined below critical levels (Proactive Value) to alert in advance and take preventive actions.

Upgrades follow change management (ITIL 2011). Monitored CIs include:

- **Physical Server**: Disk space, CPU, memory utilisation.
- **Virtual Server**: Disk space utilisation; vCPU utilisation; Allocated memory utilisation; Input/output operations/sec (IOPS).
- **Database**: DB server IOPS; DB transactions/sec.
- **Storage**: Physical storage capacity of blades; Allocated storage capacity per VM; Table space allocated to DB; Storage array hits and misses.
- **Network**: Virtual/physical server, Internet, VPN service and web services utilisation.

Capacity management includes:

- **Capacity monitoring**. Collected data is analysed to calculate the capacity in relation to current usage. Collected data is evaluated to identify needs, trends, bottlenecks, and remaining capacity to deal with increased usage.
- **Capacity forecast** based on usage growth, which is estimated in-line with project plans (e.g. application rollout), customer feedback, promotional activities, trends, etc.
- **Capacity upgrade**. The results of monitoring and forecast are compared to conclude on specific elements to be upgraded. This step also includes the activities for upgrading capacity.

4 Services

4.1 On Boarding / Off Boarding

There is no substantial on-boarding process. Upon contract award or accepted purchase order, we implement the required infrastructure configuration and deliver it to the Customer.

Regarding off-boarding, the default service assumes that the Customer will perform any data extraction and similar processes before the end of the contracted period. As soon as the contract ends, we deallocate the allocated resources considering the privacy requirements in place (e.g., permanent erasure of sensitive data).

If specific data extraction requirements are requested, we will agree to implement them as an additional service using the rates published as part of the rate card.

4.2 Service constraints

There are no service constraints. Service maintenance is scheduled outside working hours and after prior notification to the Customer if the service maintenance may disrupt the operation of the service. The service may be customised as required; however, additional setup costs may need to be charged if required.

4.3 Service Levels

4.3.1 Information Assurance

EUROPEAN DYNAMICS maintains for its hosting facilities an Information Security Management System (ISMS) certification with the ISO 27001:2013 standard. Accordingly, the Service Provider has in place all required ISMS documentation set, security policies and procedures for maintaining all collected and operational data in a secure and confidential manner within its data centre.

The security procedures and respective documentation updates are annually reviewed including the annual IT Health Check by certified Auditors who visit the Service Provider's infrastructure for this purpose.

4.3.2 Service Levels – System

The severity level of a service failure is described in the Terms and Conditions document in terms of its impact to service provision:

Table 1: Service Failures Priorities

Priority	***Description***
P1	A service failure which: 1. constitutes a total loss of availability of the system and/or operational services. 2. constitutes a loss of availability of the system and/or operational services. which has a critical impact on the activities of the users. 3. has a critical impact on the activities of the Customer. 4. causes economic loss and/or disruption to Customer. 5. results in any material loss or corruption of data.

Priority	*Description*
P2	A service failure which: 6. has a major (but not critical) adverse impact on the activities of the Customer and no work around is available
P3	A service failure which: 7. has a serious impact on the activities of the Customer which can be reduced to a moderate adverse impact due to the availability of an acceptable work around. 8. has a moderate adverse impact on the activities of the Customer
P4	A service failure which: 9. does not impact on the provision of the service to users; however, may comprise of a flaw or of a cosmetic nature and, as such, does not undermine the user's confidence in the information being displayed

P1 is the highest (i.e. most serious) severity level and P4 is the lowest (i.e., least serious) severity level.

A service failure which results in the non-availability of any part of the system shall always be classified as either a P1 or P2 service failure.

We commit to recover from any degradation of service level as soon as possible and commits to comply with the relevant Terms and Conditions document that defines the standard acknowledgement, response, and resolution of issues, as applicable.

4.3.3 Service Management Details

We have developed a customer-centred approach to guarantee the quality of the management of the services delivered. Three principles are fundamental to this approach:

- **Satisfying customers**. The company's organisation focuses on improving the level of customer satisfaction bearing in mind:
  - ◊ Customer needs, expectations, and priorities.
  - ◊ The level of customer satisfaction.
  - ◊ Available resources.

  This information is a requisite for planning improvements that will ensure customer satisfaction.
- **Involving employees**. Employees have a clear view about the way their work is structured and carried out. In many ways, they are in a better position than anyone else to see ways of improving the quality of services.

  Employees also must be able to use their own discretion and respond creatively to the needs of the Customer. Involving employees in change is a prerequisite to gaining their commitment to improvement. If employees are part of the changes and realize that they play an active role in new ways of doing things, their sense of ownership is much stronger than it is when organizations impose the change.

  For all these reasons, involving employees is critical to assuring Customer satisfaction.

- **Continuous improvement/adaptation/change**. Customer expectations change as their needs and experience evolve. Furthermore, employees continually gain new skills and find new ways of solving challenges in a creative manner. Regardless of the current level of Customer satisfaction, improvement is an ongoing task, because changes occur continuously.

The on-boarding process ensures that the Customer requirements have been fully addressed by the system and that the Customer's team operating the Service has been trained for efficient and secure operation of the Service and any existing data have been migrated to the Service, as required.

The off-boarding process ensures that the Customer will be able to extract all information maintained by the system to migrate to another Service provider. The Service Provider can support the Customer if special data extraction requirements exist.

The 3-tiered helpdesk team integrates these support services through straightforward and industry-standard processes.

4.3.4 Adherence to the EU Code of Conduct

ED's primary data centre operations are co-located in TI SPARKLE GREECE SA Tier III data centre facilities which fully comply with the EU's Code for Energy Efficient Datacentres.

The newest TI SPARKLE DATA centre (MMII) in which ED's infrastructure is co-located is the first Green Data Centre in Greece and maintains a Green Building Certification by LEED (Gold) and is powered solely from renewable sources.

The datacentre has an ISO 14001 Certification for Environmental Management, makes use of Efficient UPS with Li-ion batteries and uses LED lighting.

ED's ICT infrastructure is deployed within an APC Eco-Aisle cold-aisle containment system which manages airflow efficiently and prevents the mixing of hot and cold air, thereby enhancing cooling effectiveness and reducing energy consumption.

The data-centre provider deploys high efficiency Evaporative Free Cooling (EFC) units to cool the data-centre load, and in "free cooling" mode (when outdoor conditions permit) the units utilize ambient air for cooling without the need for mechanical refrigeration, further reducing energy consumption.

4.3.5 Service Levels – Help Desk

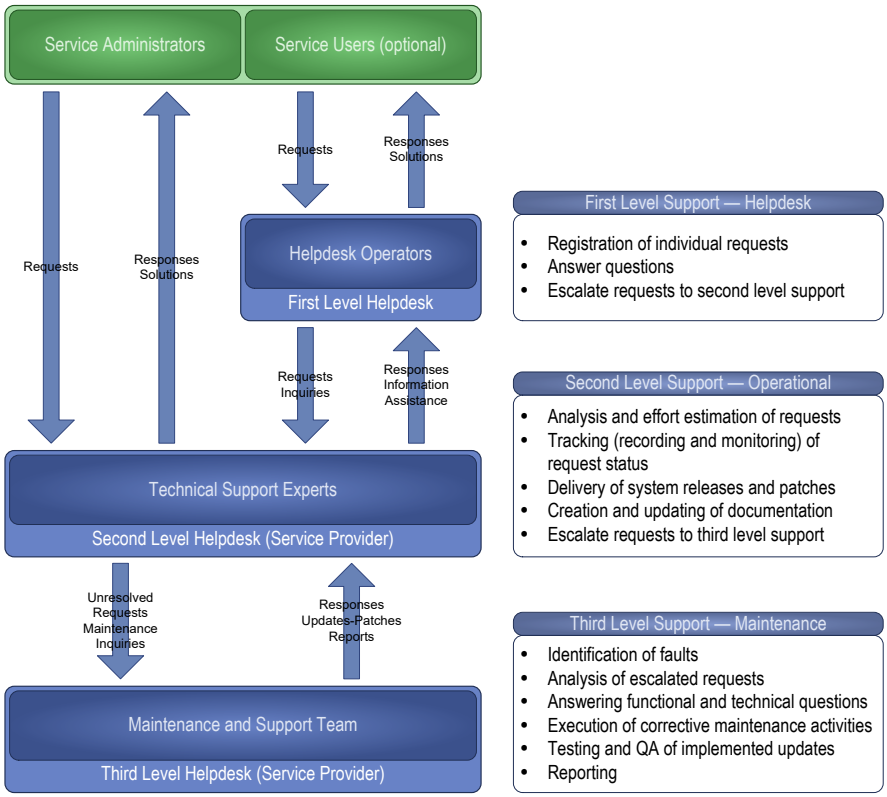
The Service Provider has established a dedicated **"Customer Support Centre"** which provides support to end-users (for assistance in using the System or reporting a fault) as required. To monitor and manage Help Desk requests, we use ServiceNow.

The Helpdesk is accessible through the following modes:

- **E-mail access:** Users can send their questions and requests by e-mail using a dedicated e-mail address.
- **Phone Access:** The users may call the Helpdesk using a UK **local phone** number.

The organisation of the Helpdesk structure to be applied for the needs of the contract encompasses of the following:

- **First level** service desk, which is directly available to End Users (if applicable).
- **Second level** service desk, which is directly available to the Customer administrators. It also receives cases that could not be resolved by the first level.
- **Third level** service desk, which is normally accessible only to the second line of helpdesk and handles incidents related to Service bugs or operational malfunctions that cannot be handled by the second line.



The Quality of Service of the Helpdesk operation will be measured based on several quality metrics. The exact measured levels of the Helpdesk's service quality agreed will be recorded in the service level agreement. As an example, typical Helpdesk service provided comply with the following standards:

- At least 75% of reported issues are resolved by the 1st Level Helpdesk support.
- At least 98% of telephone calls answered within five (5) rings (during normal operating hours).
- At least 98% of Helpdesk incidents acknowledged within ten (10) minutes (during normal operating hours).
- At least 98% of "Priority 4" incidents are resolved within 30 minutes.

The classification of incident severity (recorded in the SLA) will be used for the prioritisation of case handling.

5 Contractual matters

5.1 Pricing Overview

The pricing of the EDMAS service is provided in a separated document.

5.1.1 Volume Discounts

There are no volume discounts applicable.

5.1.2 Data Extraction Costs

If specific data extraction requirements are requested, we will agree to implement them as an additional service using the rates published as part of the rate card.

5.1.3 Data Restoration / Service Migration

Migrating services from and to the EDMAS service is a straightforward process, as presented in the on-/off-boarding process description. In addition, the Service Provider includes as an optional service element the possibility to create a complete data set in line with the Customer requirements.

5.2 Ordering and invoicing

Customers wishing to use the Service Provider's services shall follow the ordering process outlined in the G-Cloud framework agreement.

Prior to submitting the order form, the Customer and the Service Provider shall enter dialogue to determine which elements of the service will be provided. Details shall include the level of customisation/adaptation, the service package/modules, level of support, delivery of service, etc.

The initial set up fees (if applicable) will be invoiced immediately after the delivery and formal acceptance of the system on the Customer's test environment.

The payment for the recurring fees and help desk services (if applicable) will be made monthly in arrears, unless otherwise agreed.

5.3 Termination of contract

Apart from the termination terms of the G-Cloud Framework Agreement the following shall apply:

5.3.1 Termination by Customers

The Customer shall have the right to terminate the relevant Call-Off Agreement at any time by giving at least thirty (30) working days written notice.

5.3.2 Termination by Supplier

If the Customer fails to pay undisputed amounts when due, we shall notify the Customer in writing of such failure to pay. If the Customer fails to pay such undisputed sums, we may terminate the Call-Off Agreement after at least ninety (90) working days following the date of the written notice.

5.4 Technical requirements

All our relations with the Customer are described in the service provision (Call-Off) agreement, which includes the responsibilities of the Customer during the service operation.

A detailed list governing the specific service requirements for Customer responsibilities is included in the corresponding service level agreement (SLA). SLA arrangements are provided as part of the "Terms and Conditions" document.

EDMAS may only be used by users authorised by the Customer.

The Customer must not use EDMAS:

- in any way that is unlawful, illegal, fraudulent, or harmful; or
- in connection with any unlawful, illegal, fraudulent, or harmful purpose or activity.

6 Business continuity and disaster recovery

6.1 Business Continuity

EUROPEAN DYNAMICS has a Business Continuity Plan and the associated Disaster Recovery Plan (collectively the BCDR Plan) that covers its own and hosted operations. The BCDR documents all the necessary proactive/reactive actions that ensure that EDMAS are continuously provided with minimum interruption for the end-users in the event of a serious damage or catastrophe. The plan is subject to ED's change management procedures and, as such, all changes are logged; it is tested and revised biannually, regularly audited, and checked for compliance according to ISO 27001:20013 guidelines regarding physical, personnel, and procedural security and DR aspects of the EDMAS system.

A BCP is maintained by the Service Provider to ensure availability and integrity of the information and services provided by the hosting platform. The BCP is implemented according to the security controls of ISO 27001 and ensures recovery and continuity of the Managed Application Services by establishing:

- **Backup Policies & Recovery Procedures**: All critical information, system data and audit logs) are backed up daily to two backup appliances as part of the backup policy.
- **Disaster Recovery (DR) Site**: Continuity of the ICT services is achieved via the DR site. Data is continuously synchronised via redundant metro-ether fibre links to the DR site, ensuring service availability in the event of equipment/datacentre disasters.

6.1.1 Business Continuity Policy

BCP guarantees service provision in the event of incidents that may affect the premises, buildings, infrastructure, or staff. The BCP is based on ISO 27001:2013 and is re-certified annually.

All systems reported in the assets inventory of EDMAS have a successfully tested BCP, which describes the objectives, responsibilities, organisation, and actions required in the event of an incident. It is intended to be used by experts who will implement the actions defined when a decision is made to trigger the BCP. The Service Provider's BCP:

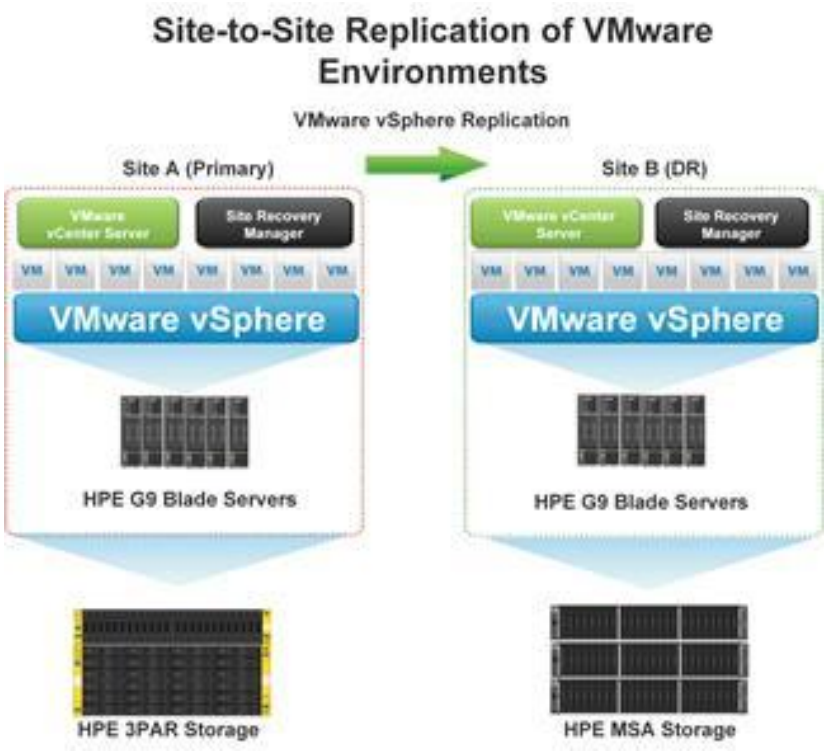
- provides effective responses, so that systems can resume normal operation in the shortest possible time (incl. backup restoration).
- contains initial and resulting damage by applying restoration measures to the affected premises, equipment, documents, and media.
- focuses on business activities.

6.1.2 Disaster Recovery Plan

Scenarios that may trigger the DR plan include failures of any critical component of the service, including server hardware, simultaneous server failure, storage array, network components, Internet WAN links, power, prevention of access to the office building and datacentre, etc.

The DR site is located fourteen miles from the primary site. A VMware platform on HPE Blade servers offers hot standby, always-on DR by synchronising data between sites. If a disaster occurs at the primary site, the DR site is promoted to Primary.

VMware Site Recovery Manager (SRM) is deployed on the two sites to orchestrate automatic migration of virtualised server environments in the event of a disaster. As illustrated, the VMs state and data are replicated continuously to the DR site via VMware vSphere Replication.



VMware SRM is an automation software integrated with an underlying replication technology to provide policy-based management, non-disruptive testing & automated orchestration of recovery plans. This provides simple and reliable recovery and mobility of virtual machines between sites with minimal or no downtime. The DR is connected to the primary site via redundant Metro-Ethernet fibre connections, redundant high-end routers with hardware encryption modules ensure that all traffic passing over the Primary-DR site connections is encrypted.

6.2 BCDR Objectives

Our business continuity objectives are:

- Provide an organised response to any disastrous incident disrupting the EDMAS service.
- Contain initial and resulting damage by early application of salvage and restoration measures.
- Provide for business continuity and survival of the company.

Our recovery objectives are:

- **Recovery Point Objective (RPO):** less than **a few seconds (usually under one second)**.
- **Recovery Time Objective (RTO):** less than **one hour (usually under 30 minutes)**. It may be adjusted to 24 hours upon request.

The RTO, from the moment of activating the DR process, includes:

- Detection & confirmation of Data Centre Failure (20 minutes)
- BGP[1] redirection of IP-space to DR Site (< 3 minutes)
- DR Database Server transition to active state (< 2 minutes)
- DNS auto-redirected to DR Site application server IP addresses (< 1 minute, in parallel to the above)

25-30 minutes is a realistic time from the BCDR plan activation through to the EDMAS service being fully available at the DR Site. The DR Site will provide the services until the return of the primary site in full operation.

[1] Border Gateway Protocol, a network routing protocol that defines how networks belonging to different administrative domains route (Internet) traffic.

6.2.1 Triggers for Activation

The following list summarises the triggers that would cause activation of the DR Site:

- **Multiple server or network component failure.**
- **Storage Array Failure:** The two controllers or two or more disks fail simultaneously.
- **Internet WAN Link Failure:** Lost connectivity to both ISPs.
- **Power Utility Failure:** Concurrent failure of the power grid, the UPS, and the generator.

6.2.2 High Availability (HA)

All key EDMAS infrastructure components are fully redundant ensuring an HA data centre architecture ideal for mission critical Managed Application Services:

- **Redundant Server Design:** all servers are fitted with redundant disks, power, and cooling.
- **Redundant Storage:** fault tolerant enterprise grade Storage Area Network solution.
- **Redundant Power**: Power outages are managed by a UPS backed up by a diesel generator.
- **Redundant Internet feeds**: The primary data centre connects via two fibre carriers to two different ISPs.

6.3 Disaster Recovery

6.3.1 Disaster Recovery Site (DRS)

The DRS of EUROPEAN DYNAMICS has the following characteristics:

- **High-speed network connection with the primary site:** A site-to-site IPSEC VPN between the DRS and primary site firewalls through a dedicated 10 Mbps FO connection.
- **High-speed connection to the internet.**
- **Compatible infrastructure with that of the primary site:** blade servers with virtualisation, SAN, backup provisions, secure networking.
- **Strong physical security:** purpose-built construction; CCTV surveillance; 24x7 security staff.

The DRS uses redundant power connections, UPS, two diesel generators, A/C, fire detection and extinguishing systems and continuous monitoring facilities.

The database server infrastructure, residing in both locations, provides support for near real-time replication of data, hence ensuring no data loss even in the case of a disaster. The overall delay for data to be replicated to the standby database, located at the secondary DR site is under one second under normal load conditions. Therefore, all EDMAS data is stored simultaneously in both the primary and secondary locations.

6.3.2 Restoration of primary site

After a disaster, the recovery of operation from the primary site is performed in the following steps:

- DR site configured as primary to enable data replication to the new primary site.
- Primary site configured to accept the replication (database logs) from the DR site.
- Data replication is conducted seamlessly for the end-users who continue to operate the EDMAS applications.
- When the replication has been completed, the two sites are switched back to their original configuration.

6.3.3 Recovery processes

Upon BCDR invocation, the EDMAS DR team members are notified and apprised of the situation through phone and email. The DR team members' contact information is documented in the Roles and Responsibilities List. The procedure for responding to incidents is detailed in the EDMAS Incident Response Policy.

To recover the EDMAS servers to their original state prior to a disaster event, an up-to-date list of all equipment and relevant information is maintained in an Asset Register. The accuracy of the register is checked annually.

In the case of a disaster that affects EDMAS helpdesk services, the Helpdesk Recovery Process focuses on the immediate identification and provision of alternative communication services by temporarily redirecting EDMAS Helpdesk phone lines to alternative off-site locations. ED VoIP infrastructure, a hybrid inter-site telephony network solution expands between the Service Provider's Headquarters and the DRS comprises VoIP PBXs, traditional PBXs, and VoIP Gateways. The relevant configuration and dial plan is kept up to date in inactive state on the VoIP PBX at the DRS, thus allowing seamless transition, as necessary.

7 Backup and restoration

The EDMAS System back-up methodology adheres to the ISO 27001 Standard requirements, allowing EDMAS to be restored in the specified time as recorded in the BCDR plan. The software used to ensure the business continuity and availability as far as backup/restore is concerned is HPE Data Protector.

Backed-up data is protected physically and environmentally to the same standards as the original data. Where backup to tape is used, all back-up media are labelled RESTRICTED and stored in an appropriate fireproof safe off site. Media reliability is assessed biannually. The data volume is monitored so that backup/restore times continue to fulfil RTO requirements. Backup to disk is also used and it is scheduled to employ also self-encrypting disks to ensure backup media protection.

Data retention follows EU and UK legal requirements. Default period for financial transaction data is seven years. Different retention periods may be defined for different data types.

7.1 Backup and Recovery Policy

A backup policy is implemented together with a DR policy. Plans ensuring availability and integrity of EDMAS data are established. Automated backups are performed and monitored.

A full and incremental backup scheme is implemented. In the event of loss, data can be recovered at any point prior to failure.

We define, in cooperation with the customer, the specific details of the backup strategy taking into consideration the following recommended specifications:

Backup schedules and retention of data:

- Daily: Incremental back-up retained for 14 days.
- Weekly: Full backup retained for 40 days.
- Monthly: Full backup retained for 6 months.
- Prior to any major software or hardware upgrade: Full backup.

7.1.1 Backup System Infrastructure

Daily automated backups of all servers are performed with HPE Data Protector backup software, backup data is stored on an HPE StoreOnce (D2D) Backup Appliance at the primary site and replicated to a second HPE StoreOnce (D2D) device at the DR site.

7.1.2 Other Provisions

Baseline configurations and "*Gold Images*" are maintained and used to deploy new systems rapidly with consistent security and to reduce human errors during deployment/configuration.

8 Service monitoring

ICT infrastructure services are delivered at a global scale, encompassing the full range of solutions *as a service* (SaaS, IaaS, PaaS) both on premise and through public/private cloud deployments. DevOps deliver operational monitoring and management services.

DevOps support operations daily. Tasks include monitoring of network and service availability, performance and security, design and provisioning of network topologies and configurations. A centralised monitoring system provides NMS monitoring, interactive and historical graphing of service statistics. Furthermore, helpdesk engineers collate relevant SLA statistics into the monthly activity reports.

8.1 Monitoring Tools

- **Nagios** is a system and network monitoring and alerting application and is used by the Service Provider to monitor hosts and services and to provide alerts to helpdesk operators via integration with Jira. Nagios is an effective tool for the extraction of accurate data related to system performance and availability.
- **LibreNMS** is a network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. The Service Provider use it to provide capacity reporting. LibreNMS offers a web interface for easy access to live graphs of server and network metrics, monitored continuously.
- The Service Provider uses **VMware vSphere** as the primary tool for managing virtualised resources. **vCenter Server** is a service acting as an administration point for VMware ESXi hosts and their network connected VMs.
- ESXi hosts allow networking, storage, and compute resources to be managed so that multiple VMs can run simultaneously on the same physical host and resources. Using **vCenter Clusters**, host resources are aggregated for better availability and utilisation. It enables features such as **vSphere HA**, **DRS** and **vMotion**.
- We use a security monitoring and alerting system in our datacentre. An **IBM QRadar SIEM** analyses and correlates security events. It examines activities across the infrastructure, incl. external threats (e.g. malware, hackers), internal threats (e.g. data breaches, fraud), risks from application flaws and configuration changes. The SIEM provides the 24x7 Security Operations Centre staff with the necessary tools and information to define filters/rules/reports, use-cases, pattern-discovery, dashboards, and data monitoring.
- The tool for recording Internet statistics is **Webalizer**. It is a web server log file analysis program that generates statistics about the visitors of the platform. Using Webalizer, it is possible to track

various parameters of site usage (e.g. visited pages, visitor geographical location, time spent, hits and unique visits) as well as perform advanced processing on collected statistics using custom visitor segmentation.

END OF DOCUMENT