REPLY

PENETRATION TESTING SERVICES

Service Definition
G-Cloud 15

REPLY
38 Grosvenor Gardens - London SW1W 0EB - United Kingdom - tel +44 (0) 207 730 6000 - fax +44 (0) 207 259 8600
infouk@reply.com

www.reply.com

TABLE of CONTENTS

SERVICE DESCRIPTION

Our Penetration Testing Service provides a comprehensive assessment of your organization's cybersecurity posture. Our team of certified ethical hackers will simulate real-world attacks to identify vulnerabilities in your systems, networks, and applications. Through rigorous testing methodologies, we aim to uncover potential security weaknesses before malicious actors do, allowing you to proactively strengthen your defence.

Our Pentesting Services are listed here:

- **Scope Definition:** The first step involves defining the scope of the penetration test. This includes determining the systems, networks, applications, and assets that will be tested. It also involves identifying the goals and objectives of the test, such as compliance requirements, specific security concerns, or critical assets to protect.
- **Information Gathering:** Penetration testers gather information about the target environment, including network architecture, IP addresses, domain names, employee information, and system configurations. This phase may involve passive techniques such as reconnaissance and open-source intelligence gathering.
- **Vulnerability Assessment:** Penetration testers scan the target systems and networks for known vulnerabilities using automated tools and manual techniques. This includes identifying outdated software, misconfigurations, weak authentication mechanisms, and other potential security weaknesses.
- **Exploitation:** Once vulnerabilities are identified, penetration testers attempt to exploit them to gain unauthorized access to the target systems or sensitive data. This phase involves simulating real-world attack scenarios, such as launching SQL injection attacks against web applications or exploiting misconfigured network devices.
- **Privilege Escalation:** If initial access is achieved, penetration testers attempt to escalate privileges to gain deeper access to the target environment. This may involve exploiting weaknesses in access control mechanisms, exploiting misconfigured permissions, or leveraging compromised credentials.
- **Documentation:** Throughout the testing process, penetration testers document their findings, including the vulnerabilities discovered, the exploitation techniques used, and the potential impact on the organization's security. This documentation serves as the basis for the final penetration testing report.
- **Reporting and Remediation:** Upon completion of the penetration test, the findings are compiled into a detailed report, which includes an executive summary, a technical analysis of vulnerabilities, and prioritized recommendations for remediation. The organization can then use this information to address security weaknesses and strengthen its defences.
- **Follow-Up and Support:** The penetration testing service provider may offer post-assessment support, including consultation to discuss the findings, guidance on remediation efforts, and assistance with implementing security best practices. This ensures that the organization can effectively address identified vulnerabilities and improve its overall cybersecurity posture.

Reply's Dynamic Penetration Testing Solutions

Infrastructure Penetration Testing

We offer Infrastructure Security Penetration Testing service for both external and internal network components. Our tailored packages are available to address the specific security needs of your organization, covering a range of infrastructure elements and configurations.

External Network Security Assessment:

- Identification of vulnerabilities in externally facing network devices, including firewalls, routers, and web servers.
- Evaluation of perimeter defences to detect potential entry points for cyber threats.

- Analysis of internet-facing services and protocols for weaknesses and misconfigurations.
- Assessment of remote access mechanisms, such as VPNs and remote desktop services.
- Detailed reporting on identified vulnerabilities, risk levels, and recommended remediation actions.

Internal Network Security Assessment:

- Examination of internal network devices, servers, and workstations for security vulnerabilities.
- Analysis of network segmentation and access controls to prevent unauthorized access to sensitive resources.
- Review of internal communication protocols and traffic patterns for potential security risks.
- Assessment of user privileges and account management practices to mitigate insider threats.
- Comprehensive reporting on internal network vulnerabilities, including prioritized recommendations for remediation.

Key Assets and Details:

- External Network Assets: Internet-facing devices, web applications, VPN endpoints, DNS servers, email servers, and other externally accessible resources.
- Internal Network Assets: Servers, workstations, network devices (e.g., switches, routers), databases, file shares, printers, and other internal infrastructure components.
- Infrastructure Details: IP addresses, domain names, network diagrams, system configurations, firewall rulesets, and access control lists (ACLs).

We offer these Infrastructure Pentesting Service Packages:

Basic Package:

- External Penetration Testing: Assessment of external-facing infrastructure components to identify vulnerabilities exploitable by external threat actors.
- Utilization of automated scanning tools to identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), and misconfigurations.
- Compilation of a concise report outlining identified vulnerabilities and recommended remediation actions.

Standard Package:

- ***External and Internal Penetration Testing:*** Evaluation of both external-facing and internal network devices, servers, and workstations for security vulnerabilities.
- ***Vulnerability Assessment:*** Combination of automated scanning tools and manual testing techniques to identify a wider range of vulnerabilities.
- ***Detailed Reporting:*** Compilation of a detailed report detailing identified vulnerabilities, risk levels, and recommended remediation actions, with prioritization based on severity.

Advanced Package:

- ***External and Internal Penetration Testing:*** Comprehensive assessment of external-facing and internal network infrastructure components, including user privileges and account management practices.
- ***Exploitation and Proof of Concept:*** Demonstration of the impact of identified vulnerabilities through exploitation and proof-of-concept scenarios.
- ***Advanced Reporting:*** Compilation of an in-depth report detailing identified vulnerabilities, exploitation techniques, and actionable insights for remediation, with executive summaries and technical details for stakeholders at all levels.

Web Application Penetration Testing

Web Application Penetration Testing is essential for ensuring the security and integrity of your web-based software solutions. Our comprehensive service offers a systematic approach to identifying and addressing vulnerabilities within your web applications, thereby minimizing the risk of exploitation by malicious actors.

Discovery Phase:

- Understanding the application's architecture, functionality, and technology stack.
- Identifying entry points and potential attack surfaces, including input fields, authentication mechanisms, and data transfer channels.
- Analysing the application's business logic and workflows to identify potential security flaws.

Reconnaissance:

- Conducting reconnaissance to gather information about the application, such as URLs, endpoints, and technologies used.
- Identifying potential vulnerabilities and attack vectors based on the information gathered.

Vulnerability Assessment:

- Performing both automated and manual vulnerability scans to identify common security flaws, such as SQL injection, cross-site scripting (XSS), and authentication bypass.
- Analysing the results of vulnerability scans to prioritize and validate identified issues.

Exploitation and Proof of Concept:

- Exploiting identified vulnerabilities to demonstrate their impact and potential risks to the application.
- Developing proof-of-concept (PoC) exploits to illustrate the exploitation process and provide actionable evidence to stakeholders.

Reporting and Remediation:

- Compiling a detailed report summarizing the findings of the penetration test, including identified vulnerabilities, risk levels, and recommended remediation actions.
- Providing guidance and recommendations for remediation efforts, including code fixes, configuration changes, and security best practices.
- Collaborating with development teams and stakeholders to prioritize and address identified security issues.

Key Components

- **Black-box Testing:** Assessing the application from an external perspective without prior knowledge of its internal workings.
- **White-box Testing:** Evaluating the application with full access to its source code, architecture, and design documentation.
- **Gray-box Testing:** Combining elements of both black-box and white-box testing to simulate an insider or privileged attacker perspective.

Service Package:

Basic Package:

- Utilization of automated scanning tools to identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure configurations.
- Conducting basic tests on critical web application functionalities to identify common security flaws.
- Compilation of a concise report outlining identified vulnerabilities and recommended remediation actions.

Standard Package:

- Combination of automated scanning tools and manual testing techniques to identify a wider range of

vulnerabilities and security issues.

- Comprehensive assessment of critical web application functionalities, including authentication mechanisms, input validation, and session management.
- Compilation of a detailed report detailing identified vulnerabilities, risk levels, and recommended remediation actions, with prioritization based on severity.

Advanced Package:

- Utilization of advanced testing methodologies and techniques to identify complex security vulnerabilities, including business logic flaws and authorization bypass techniques.
- Demonstration of the impact of identified vulnerabilities through exploitation and proof-of-concept scenarios.
- Executive Summary and Technical Details: Compilation of an executive summary for stakeholders and detailed technical documentation for developers and IT teams, providing actionable insights for remediation efforts.

Mobile Application Testing

Mobile Application Penetration Testing is essential for ensuring the security of your iOS and Android apps against cyber threats. Our specialized service offers targeted assessments tailored for both platforms, providing comprehensive protection for your mobile applications.

1. **Platform-Specific Analysis:**
    a. iOS: Examination of the application's architecture, APIs, and security features unique to the iOS platform.
    b. Android: Analysis of the app's APK file, libraries, and platform-specific security controls inherent to the Android ecosystem.
2. **Reverse Engineering:**
    a. iOS: Decompilation and analysis of the IPA file to understand the app's logic, data storage mechanisms, and encryption methods.
    b. Android: Reverse engineering of the APK file to uncover vulnerabilities related to code obfuscation, insecure storage, and improper permission handling.
3. **Static and Dynamic Analysis:**
    a. iOS: Static analysis of the Objective-C or Swift code to identify potential security flaws, such as insecure data storage and insufficient input validation.
    b. Android: Static analysis of the Java code to uncover vulnerabilities, including improper certificate validation, insecure data transmission, and vulnerable third-party libraries.
4. **Device Emulation and Testing:**
    a. iOS: Dynamic analysis of the running app on a jailbroken device or emulator to simulate real-world attack scenarios, such as jailbreak detection bypass and runtime manipulation.
    b. Android: Dynamic analysis of the app on a rooted device or emulator to assess security controls, including runtime permission checks, secure inter-process communication, and sandboxing.
5. **Reporting and Remediation:**
    a. Compilation of a detailed report outlining identified vulnerabilities, risk levels, and recommended remediation actions specific to each platform.
    b. Guidance and recommendations for remediation efforts, including code fixes, configuration changes, and security best practices tailored for iOS and Android.

Service Packages:

Basic Package:

- Essential vulnerability assessment targeting common security flaws prevalent in iOS and Android

apps.

- Identification of platform-specific vulnerabilities, such as insecure data storage, inadequate encryption, and insufficient input validation.
- Suitable for start-ups and small businesses developing mobile apps for iOS and Android platforms.

Standard Package:

- Comprehensive assessment covering a wider range of vulnerabilities and attack vectors specific to iOS and Android.
- In-depth analysis of platform-specific security controls, including iOS App Transport Security (ATS), Android App Permissions, and secure inter-process communication.
- Ideal for medium-sized enterprises looking to enhance the security posture of their mobile apps on both iOS and Android platforms.

Advanced Package:

- Advanced testing methodologies and techniques for complex and highly regulated environments, offering platform-specific insights and recommendations.
- Deep dive into platform-specific security mechanisms, including iOS Keychain Services, Android Secure Storage, and runtime permission models.
- Tailored for large enterprises, government agencies, and organizations with stringent security requirements for mobile apps on iOS and Android platforms.

API Penetration Testing

API Penetration Testing is critical for ensuring the security of your application programming interfaces (APIs) against cyber threats. Our specialized service offers a systematic approach to identifying and mitigating vulnerabilities within your APIs, providing comprehensive protection for your digital assets.

1. **API Discovery and Analysis:**
    a. Identification of all APIs used in your application ecosystem, including RESTful, SOAP, and GraphQL APIs.
    b. Analysis of API documentation, endpoints, methods, parameters, and authentication mechanisms.
2. **Threat Modeling:**
    a. Identification of potential attack vectors and security risks associated with each API, considering input validation, authentication, authorization, and data integrity.
3. **Vulnerability Assessment:**
    a. Conducting both manual and automated testing to identify common API vulnerabilities, such as injection attacks, insecure authentication, broken access controls, and sensitive data exposure.
    b. Analysis of API responses, error handling, and data validation to uncover security weaknesses and implementation flaws.
4. **Security Testing:**
    a. Simulating real-world attack scenarios, such as SQL injection, XML external entity (XXE) attacks, and cross-site scripting (XSS), to assess the robustness of API security controls.
    b. Testing for rate limiting, throttling, and other mechanisms to prevent abuse and denial-of-service (DoS) attacks.
5. **Reporting and Remediation:**
    a. Compilation of a detailed report outlining identified vulnerabilities, risk levels, and recommended remediation actions for each API.
    b. Providing guidance and recommendations for remediation efforts, including code fixes, configuration changes, and security best practices to enhance API security.

Service Packages:

Basic Package:

- Essential vulnerability assessment targeting common API security flaws prevalent in RESTful and SOAP APIs.
- Identification of vulnerabilities, such as injection attacks, broken authentication, and insecure direct object references.
- Suitable for startups and small businesses developing APIs for internal or external use.

Standard Package:

- Comprehensive assessment covering a wider range of API vulnerabilities and attack vectors, including GraphQL APIs and API gateway security.
- In-depth analysis of authentication mechanisms, authorization controls, and data validation practices.
- Ideal for medium-sized enterprises with multiple APIs exposed to internal and external stakeholders.

Advanced Package:

- Advanced testing methodologies and techniques for complex and highly regulated environments, offering in-depth analysis of API security controls and architecture.
- Deep dive into business logic flaws, access control vulnerabilities, and secure API design principles.
- Tailored for large enterprises, government agencies, and organizations with mission-critical APIs handling sensitive data and transactions.

CREST OVS Web App Assessment

The CREST OVS (OWASP Verification Standard) Web Application Assessment is a comprehensive security evaluation methodology developed by CREST, leveraging the OWASP ASVS (Application Security Verification Standard). This assessment offers a detailed examination of your web applications, including their underlying server and operating system, to identify and mitigate security risks effectively.

Comprehensive Vulnerability Discovery:

- Examination of your web applications to discover vulnerabilities before they can be exploited.
- In-depth analysis of the application's architecture, source code, and underlying infrastructure.

Detailed Approach to Security:

- Assessment of your processes and source code to identify potential security risks and weaknesses.
- Evaluation of application processes and documentation to ensure adherence to security best practices.

Two Levels of Assessment:

- **CREST OVS Level 1**: Utilizes the ASVS tier one methodology, focusing on overall application security without requiring access to source code.
- **CREST OVS Level 2**: Utilizes the ASVS level two methodology, offering an even deeper assessment that may require access to source code and detailed documentation.

Key Features:

- Find Critical Weaknesses
- Assess Your Source Code
- Review Application Processes
- In-Depth Web App Test

Reporting and Documentation Guidelines

The purpose of our penetration testing reports is to assist organizations in enhancing their security posture by identifying areas of potential risk that may require remediation. Our reports are structured to clearly communicate what was tested, how it was tested, and the results of the testing process.

Identified Vulnerability Reporting:

- Reply's reports include a discussion of the steps, vectors, and exploited vulnerabilities that led to penetration during testing, as well as vulnerabilities posing potential risks to the environment.
- Examples of identified vulnerabilities that were not exploited but are included in the report are firewall misconfigurations and detection of credentials obtained through web-application error messages.

Assigning a Severity Score:

- To prioritise remediation efforts, a severity or risk ranking is assigned to each detected security issue during the reporting phase.
- We utilize industry-standard references such as the NVD, Common Vulnerability Scoring System (CVSS), Common Weakness Enumeration (CWE), and others to assign severity scores.
- Custom scoring may be applied, and our reports provide a traceable set of reasoning for any modifications made to industry-standard scores.

Penetration Test Report Outline

1. Executive Summary
    a. Brief overview of the penetration test scope and major findings.
2. Statement of Scope
    a. Detailed definition of the network and systems tested, including delineation of CDE vs. non-CDE systems.
    b. Identification and explanation of critical systems included in the test as targets.
3. Statement of Methodology
    a. Description of methodologies used for testing, such as port scanning and Nmap.
4. Statement of Limitations
    a. Documentation of any testing restrictions, such as designated hours or bandwidth limitations.
5. Testing Narrative
    a. Detailed account of testing methodology and progression, including challenges encountered and how they were addressed.
6. Segmentation Test Results
    a. Summary of testing performed to validate segmentation controls, if applicable.
7. Findings
    a. Explanation of vulnerabilities, including potential exploitation methods, risk ranking, affected targets, and references.
    b. References may include CVE, CWE, BID, OSBDB, etc.
    c. Tools Used
    d. List of tools utilized during testing.
8. Cleanup Instructions
    a. Directions on post-penetration test cleanup tasks, such as removing test accounts or database entries and restoring security controls.

Retesting Considerations and Report Outline

1. Executive Summary

    Summary of retest findings and outcomes.

2. Dates

    Original test date and retest date.

3. Original Findings

Summary of vulnerabilities identified in the original test.

4. Results of Retest

Outcome of retesting efforts, including resolution of identified vulnerabilities and any remaining issues.

ONBOARDING

Reply provide a seamless onboarding process for our penetration testing service, starting with an initial consultation to understand the client's objectives and scope requirements. Collaboratively, we define the engagement's parameters and document them in a detailed proposal, ensuring transparency and alignment. During the preparation phase, we work closely with the client to gather necessary information and access credentials for smooth execution. Our expert team then conducts thorough penetration testing, utilizing automated tools and manual techniques to identify vulnerabilities across networks, applications, and systems. Following analysis, we provide a comprehensive report detailing findings and recommended remediation steps. Through a scheduled presentation, we guide the client through the report's insights, offering prioritized remediation guidance. Our support extends beyond reporting, providing ongoing assistance to address vulnerabilities effectively. Continuous feedback and improvement ensure our services remain tailored and effective, maintaining robust security measures for our clients.

Offboarding

Ensuring a secure exit or transition process is crucial for maintaining the integrity of the client's systems and data. Here's how Reply handle the offboarding or transition to another supplier:

- Exit Strategy Development: At the onset of the engagement, we collaborate with the client to develop an exit strategy outlining the steps for termination or transition. This includes defining roles, responsibilities, timelines, and communication channels.
- Data Backup and Transfer: Prior to offboarding, we assist the client in securely backing up their data, ensuring that all critical information is preserved and accessible. If necessary, we facilitate the transfer of data to the client or the new service provider using encrypted channels and protocols.
- Access Revocation: We systematically revoke access to our systems, tools, and networks, ensuring that no unauthorized access remains after the engagement concludes. This includes deactivating user accounts, removing privileged access, and revoking any permissions granted during the engagement.
- Documentation Handover: We provide comprehensive documentation detailing the findings, remediation steps, and any other relevant information to the client or the new service provider. This ensures continuity of security efforts and facilitates a smooth transition.
- Knowledge Transfer: If the client transitions to another service provider, we offer knowledge transfer sessions to familiarize them with the systems, processes, and tools used during the engagement. This helps minimize disruptions and ensures continuity of security measures.
- Closure Meeting: We conduct a closure meeting with the client to review the engagement, discuss any outstanding issues or concerns, and obtain feedback on our services. This allows us to address any remaining issues and ensure client satisfaction.
- Post-Engagement Support: Following the offboarding or transition, we remain available to provide post-engagement support and address any additional questions or concerns that may arise. Our goal is to ensure a seamless transition and maintain a positive relationship with the client.

Access to Data

Ensuring secure access to client data upon exit is paramount to maintaining confidentiality and integrity. We begin by conducting a comprehensive inventory of all client data stored within our systems, encrypting it both in transit and at rest using industry-standard protocols. Strict access controls and authentication mechanisms are implemented to restrict access to authorized personnel only, with permissions regularly reviewed and updated. Client data is segregated from other data within our systems, ensuring isolation and protection. Upon exit, all access rights to client data are promptly revoked, including user account deactivation and permission removal. If requested, we securely delete or anonymize client data in accordance with retention policies and regulatory requirements. Detailed documentation and audit trails of data access are maintained, providing transparency and accountability. Before exiting, we verify with the client that all necessary data access has been revoked. Finally, we adhere to legal and regulatory obligations regarding data protection and privacy, ensuring compliance with contractual agreements and

applicable laws such as GDPR or HIPAA. Through these measures, we ensure that client data remains secure throughout the exit process, mitigating the risk of unauthorized access or data breaches.

SECURITY

Personnel Security

As a Specialist Cloud Service, the capability being offered is not limited to specific Impact levels (as it is not infrastructure, software or a platform) and can be used, subject to personal Security Clearance levels.

Reply consultants are mostly Security Cleared (SC), some have higher-level Developed Vetting (DV) clearances. We also have a pool of NPPV3 Consultants for Policing work. The majority of our work for both public and private sector clients is at IL2 but we work in the Official, Secret and Top-Secret domains.

Our hard and soft information security processes have been designed and approved by independent CESG CLAS accredited consultants.

Information Security

We are ISO27001, Cyber Essentials certified and our Quality Assurance processes are based upon and compliant with our ISO 9001 accreditation. Our Information Security processes are directly guided by our ISO27001 accreditation. We shall adhere to local information and other security policies and will apply local Security Operating Procedures (SyOPs) as may exist. If such do not exist we shall apply our own SyOPs.

Physical Security

The Main Reply Office (London, UK) is a Police Accredited Secure Facility (PASF) with access controls for each point of entry. All Laptops/Phones must be stored securely overnight. When working on a client-site our consultants adhere to client security policies.

TRAINING & KNOWLEDGE TRANSFER

Training and knowledge transfer are integral parts of our service delivery process. Reply provide comprehensive training sessions tailored to your team's needs, covering topics such as best practices in cybersecurity, threat detection, and incident response. These sessions are conducted by our experienced professionals, who share insights, strategies, and techniques to enhance your team's capabilities in managing security risks effectively. Additionally, we offer ongoing support and access to resources such as documentation, tutorials, and workshops to ensure continuous learning and development. Our goal is to empower your team with the knowledge and skills needed to address cybersecurity challenges confidently and proactively.

ORDERING AND INVOICING PROCESS

To begin the process, please contact glue.frameworks@reply.com with details of your organisation, role and high-level requirements.

Our Framework Manager will connect you to our experts and from here we will organise an introductory discussion to go into more detail and shape a proposed engagement that suits your needs.

We invoice for both fixed price and time and materials engagements one month in arrears. For fixed price engagements, this takes place upon completion of the deliverable(s), or in stages, if the size of the engagement is greater than £40,000 excluding VAT.

Payment terms are 30 days net of receipt of invoice.

CUSTOMER RESPONSIBILITIES

To ensure successful delivery of our Penetration Testing Services, we require the following from our customers:

1. **Access and Permissions:** Provide necessary access credentials, permissions, and documentation for all relevant systems, networks, and applications to facilitate testing.
2. **Scope and Objectives:** Clearly define the scope and objectives of the penetration testing engagement, including specific areas to be tested, testing methodologies to be employed, and desired outcomes.
3. **Communication and Collaboration:** Maintain open communication channels throughout the engagement, including regular meetings, status updates, and feedback sessions to ensure alignment with expectations.
4. **Resource Availability:** Make available the necessary resources, including personnel, tools, and infrastructure, to support the testing process and facilitate remediation efforts.
5. **Documentation and Documentation:** Provide documentation related to network architecture, system configurations, application functionalities, and any relevant security controls to aid in the testing process.
6. **Cooperation and Coordination:** Collaborate with our team to schedule testing activities, coordinate with internal stakeholders, and address any issues or concerns that may arise during the engagement.
7. **Commitment to Remediation:** Demonstrate a commitment to addressing identified vulnerabilities and implementing recommended remediation actions in a timely manner to enhance overall security posture.

By ensuring collaboration, communication, and cooperation between our team and the customer, we can effectively deliver our Penetration Testing Services and help strengthen the organization's cybersecurity defenses.

ABOUT REPLY

Reply is a company that specialises in Consulting, Systems Integration and Digital Services with a focus on the conception, design and implementation of solutions based on the new communication channels and digital media.

Reply partners with key industrial groups in defining and developing business models made possible by the new technological and communication paradigms such as Artificial Intelligence, Big Data, Cloud Computing, Digital Communication, the Internet of Things and Mobile and Social Networking. In so doing, it aims to optimise and integrate processes, applications and devices.

Reply's offer is aimed at fostering the success of its customers through the introduction of innovation along the whole economic digital chain. Given its knowledge of specific solutions and due to a consolidated experience, Reply addresses the main core issues of the various industrial sectors.

Through its network of specialist companies, Reply supports some of Europe's leading industrial groups in Telco & Media, Industry & Services, Banks & Insurance, and Public Administration to define and develop business models, suited to the new paradigms of Artificial Intelligence, Big Data, Cloud Computing, Digital Media and the Internet of Things.

We make innovation happen.

We started with a small team and a purpose: to help the digital revolution happen. Today, we are a team of more than 14,600 people in 16 different countries but we still have the same DNA, made up of agile, vertical task forces and an inner passion for innovation.

We are a decentralised network of specialised companies.

Among Replyers, you will find passionate geeks, visionary strategists, and creative minds, each with sharp skills in a specific business, who cooperate together and never stop learning from each other.

Make forward, act sustainably.

We know a sustainable future is possible and technology can be a strong asset to reach it. As leaders in digital transformation, we push for change and operate in full accordance with the highest ethical standards and with respect for the rights of future generations