Google IT Professional Support Certificate:

Overview and Course Information

About the Certificate

The Google IT Support Professional Certificate is a program that helps people prepare for entry-level roles in IT support with no experience or degree necessary. Through a dynamic mix of video lectures, quizzes, and hands-on labs and widgets, the Google IT Support Professional Certificate introduces learners to troubleshooting, customer service, networking, operating systems, system administration, and security. The curriculum includes motivating personal stories from Google employees, with unique backgrounds and perspectives, who started their careers in IT support. Upon completion of the certificate, learners receive a Google IT Support Professional Certificate badge they can display on their LinkedIn profiles.

Course Overview

There are the five courses in the program; an overview of each is provided below. For additional information, please consult the Coursera website.

1. *Technical Support Fundamentals*

This course is the first of a series that aims to prepare you for a role as an entry-level IT Support Specialist. In this course, you'll be introduced to the world of Information Technology, or IT. You'll learn about the different facets of Information Technology, like computer hardware, the Internet, computer software, troubleshooting, and customer service. This course covers a wide variety of topics in IT that are designed to give you an overview of what's to come in this certificate program.

By the end of this course, you'll be able to: ● understand how the binary system works. ● assemble a computer from scratch. ● choose and install an operating system on a

computer. ● understand what the Internet is, how it works, and the impact it has in the modern world. ● learn how applications are created and how they work under the hood of a computer. ● utilize common problem-solving methodologies and soft skills in an Information Technology setting.

2. The Bits and Bytes of Computer Networking

This course is designed to provide a full overview of computer networking. We'll cover everything from the fundamentals of modern networking technologies and protocols to an overview of the cloud to practical applications and network troubleshooting.

By the end of this course, you'll be able to: ● describe computer networks in terms of a five-layer model. ● understand all of the standard protocols involved with TCP/IP communications. ● grasp powerful network troubleshooting tools and techniques. ● learn network services like DNS and DHCP that help make computer networks run. ● understand cloud computing, everything as a service, and cloud storage.

3. Operating Systems and You: Becoming a Power User

In this course -- through a combination of video lectures, demonstrations, and hands-on practice -- you'll learn about the main components of an operating system and how to perform critical tasks like managing software and users and configuring hardware.

By the end of this course you'll be able to: ● navigate the Windows and Linux filesystems using a graphical user interface and command line interpreter. ● set up users, groups, and permissions for account access. ● install, configure, and remove software on the Windows and Linux operating systems. ● configure disk partitions and filesystems. ● understand how system processes work and how to manage them. ● work with system logs and remote connection tools. ● utilize operating system knowledge to troubleshoot common issues in an IT Support Specialist role.

4. System Administration and IT Infrastructure Services

This course will transition you from working on a single computer to an entire fleet. Systems administration is the field of IT that's responsible for maintaining reliable computers systems in a multi-user environment. In this course, you'll learn about the infrastructure services that keep all organizations, big and small, up and running. We'll deep dive on cloud so that you'll understand everything from typical cloud infrastructure setups to how to manage cloud resources. You'll also learn how to manage and configure servers and how to use industry tools to manage computers, user information,

and user productivity. Finally, you'll learn how to recover your organization's IT infrastructure in the event of a disaster.

By the end of this course you'll be able to: ● utilize best practices for choosing hardware, vendors, and services for your organization. ● understand how the most common infrastructure services that keep an organization running work, and how to manage infrastructure servers. ● understand how to make the most of the cloud for your organization. ● manage an organization's computers and users using the directory services, Active Directory, and OpenLDAP. ● choose and manage the tools that your organization will use. ● backup your organization's data and know how to recover your IT infrastructure in the case of a disaster. ● utilize systems administration knowledge to plan and improve processes for IT environments.

5. IT Security: Defense Against the Digital Dark Arts

This course covers a wide variety of IT security concepts, tools, and best practices. It introduces threats and attacks and the many ways they can show up. We'll give you some background of encryption algorithms and how they're used to safeguard data. Then, we'll dive into the three "A's" of information security: authentication, authorization, and accounting. We'll also cover network security solutions, ranging from firewalls to WIFI encryption options. Finally, we'll go through a case study, where we examine the security model of Chrome OS. The course is rounded out by putting all these elements together into a multi-layered, in-depth security architecture, followed by recommendations on how to integrate a culture of security into your organization or team.

At the end of this course, you'll understand: ● how various encryption algorithms and techniques work as well as their benefits and limitations. ● various authentication systems and types. ● the difference between authentication and authorization. ● how to evaluate potential risks and recommend ways to reduce risk. ● best practices for securing a network. ● how to help others to grasp security concepts and protect themselves.